GENESYS

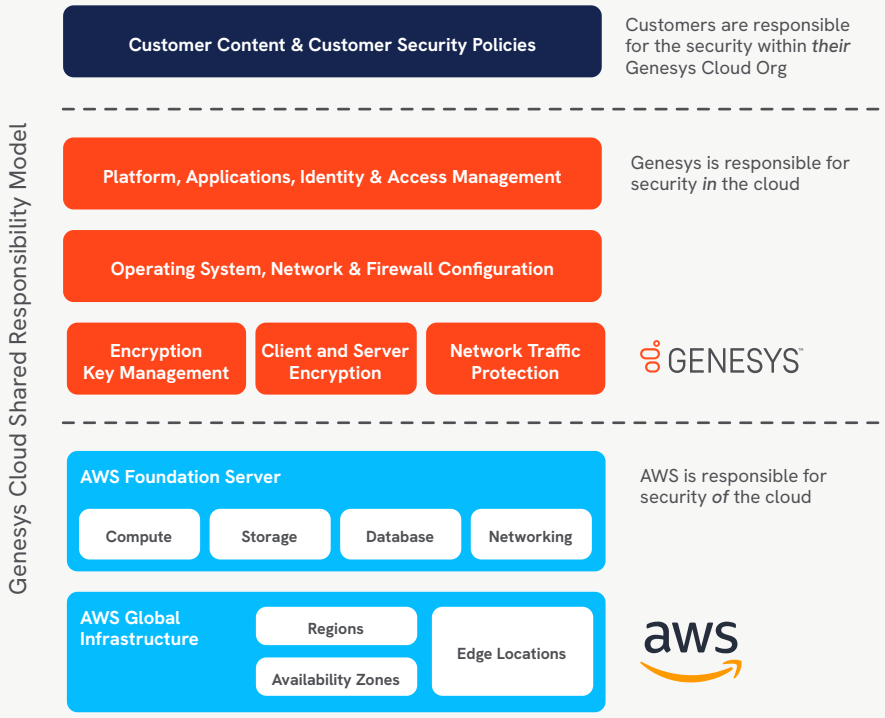
Genesys Cloud

Security and compliance overview

The security of our service is instrumental in maintaining the trust our customers place in Genesys. Our comprehensive approach to security is based on the principles of informed oversight, effective risk management, consistent security practices, rigorous audits and continuous feedback. Our top priority is to keep your data secure and your business protected — so you can have peace of mind.

Shared responsibility model

Managing security and compliance is a shared responsibility between Genesys, our cloud service provider and our customers/partners. Amazon Web Services (AWS) operates and manages the security and compliance *of* the cloud computing infrastructure. Genesys manages security *in* the cloud. And the end customer/partner is responsible for security within *their* Genesys Cloud™ organization. This distribution of responsibilities can help relieve the customer's operational burden and, in many cases, offers higher standards of security than most organizations can achieve in-house .



Genesys security controls

Genesys follows an information security management system (ISMS) that's based on ISO standards for security policies, processes and controls focused on maintaining a secure environment with maximum oversight. Additionally, our controls governing the availability, confidentiality and security of customer data are SOC 2 Type 2 compliant.

To maintain the confidentiality, integrity and availability of data and services, Genesys uses a defense-in-depth strategy. This approach implements multiple layers of security mechanisms and controls so that if one control fails or a vulnerability is exploited, another is in place to help mitigate the risk.

The following sections provide a high-level overview of our security strategy, protocols and controls. This content doesn't represent our full security posture and is intended as a starting point for broader and deeper discussions.

Organizational security

InfoSec team: Genesys employs a full-time Information Security and Compliance team that's focused on security, auditing, compliance and risk management. This team works in conjunction with the Security Steering Committee to ensure oversight and governance, as well as with HR, Legal, Operations and Engineering teams to ensure the Cloud Security Policy is enforced and operates effectively.

Training: Employees and contractors must pass security training; employees are required to recertify for security and compliance training on an annual basis. This includes annual compliance; information security; privacy; HIPAA security and privacy; and PCI training. Access to the Genesys code repository requires additional annual training in secure development.

Physical security

Data center: AWS provides data center security. Controls include perimeter security such as fencing, walls, security staff, video surveillance and intrusion detection systems. Authorized staff must pass two-factor authentication to access data center floors. Full compliance documentation is publicly available on the AWS Cloud Compliance site.

Workplace: Access to Genesys offices is restricted and controlled by security badges. Visitors must be escorted by an employee.

Network security

Approach: AWS provides a strong foundation of security and compliance that Genesys supplements by employing industry standard network security controls designed to protect customer data. Genesys Cloud follows AWS best practices for the security group, load balancer and routing configurations.

Logical separation: The production environment within AWS where the Genesys Cloud services and customer data are hosted is logically isolated in a Virtual Private Cloud (VPC).

Data connections: All connections between the Genesys Cloud VPC and browsers, mobile apps and other components are secured via HTTPS and TLS 1.2 over the public internet.

Firewall: All Genesys Cloud server instances are behind AWS Security Group firewalls. These firewalls have granular ingress and egress IP/port restrictions between server instance groups to each other and the internet.

DDoS: AWS Shield is a managed Distributed Denial-of-Service (DDoS) protection leveraged in Genesys Cloud. Genesys Cloud follows AWS best practices for DDoS protection. Genesys Cloud also consumes many services that are resilient, such as Route53, ASGs, ELBs and CloudFront. Further, Genesys Cloud operates within a VPC with granular security groups to control ingress points and limit our attack surface.

Data security

Encryption: Genesys Cloud supports encryption of data both in transit and at rest. In transit, this is supported by strong cryptography, most notably TLS 1.2 or higher. All encryption for data at rest is AES 256-based. Data is encrypted with a combination of different technologies within the platform, which include but are not limited to Object Level encryption, SSE and Root File system encryption.

Recordings: Sensitive data such as call recordings are encrypted at the point of recording with customer-specific keys, encrypted in transport with TLS and again encrypted at REST with Amazon S3 SSE.

Voice: Encrypted voice traffic uses TLS (SIP signaling) and SRTP (IP voice).

Data isolation: Multitenant logical separation is enforced by tagging system events with the associated unique Org ID. Genesys Cloud services and APIs honor these tags to ensure that customer data remains isolated from other customers' data.

Data control: Customers can easily export or delete their data through our API.

Identity and access control

Authorization: Access permissions to our cloud environment use the least-privilege principle and role-based access control mechanisms. Access is highly restricted based on job role.

Authentication: Genesys authorized users access the cloud environment using multifactor authentication. All user activities are logged and monitored.

Operational security

Vulnerability scanning: Genesys scans continuously for security threats using commercially tested tools, penetration testing and pre-deployment testing. Findings are immediately logged, evaluated, prioritized and assigned for prompt remediation.

Intrusion detection: Genesys has implemented and maintains a host-based intrusion detection system and network-based intrusion detection system designed to provide alerts in the event of suspicious activity.

Malware: Genesys proactively monitors our systems for malware through host-based intrusion detection, File Integrity Monitoring (FIM) tools and anti-malware. We also monitor system access and command use.

Application security

Secure by design: Security is embedded in the Software Development Lifecycle (SDLC) at Genesys. Independent product security team members ensure new features go through security code reviews and vigorous security testing prior to release.

Training: Development teams are regularly trained on web application security, including, but not limited to, Open Web Application Security Project (OWASP) Top 10 and SANS Top 25. Code testing methods include Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Software Composition Analysis (SCA).

Quality assurance: Testing is an iterative process involving multiple layers, including unit tests, integration tests, automated user interface tests, automated API tests and performance testing. We also follow chaos principles by injecting intentional failures into our non-production environments to ensure our services can tolerate them. Further, we commission a bug bounty program with HackerOne to surface any other vulnerabilities.

Change management: Documented change management procedures govern how changes to the Genesys Cloud platform are requested, reviewed, approved, tested and implemented into production. Production is an immutable environment. Changes must be made in lower environments and pushed to production. This approach improves reliability by guaranteeing the systems tested in pre-production are functionally identical to those deployed in production.

Product security

Logins: The password complexity is definable and can include minimum length, letters, numbers, special characters and time-based change. All passwords are hashed using a salt with SHA□512 combined with PBKDF2. Single sign-on (SSO) is supported with leading identity providers or any SAML 2.0 compliant provider.

Multi-factor authentication: Administrators can enable native multi-factor authentication (MFA) for Genesys Cloud users to increase security and reduce the risk of fraud. MFA requires users to enter a code from their phone or another device in addition to their password when logging in to Genesys Cloud.

Access: Access is configured to the user level based on roles and permissions. Roles and responsibilities are segregated based on functional requirements and least privilege principles. In addition, admins can use Divisions to group and segregate objects while keeping them inside the same organization.

IP whitelisting: Administrators can limit access to their Genesys Cloud Org to only those users connecting from specific IP addresses.

Audit log: Audit events provide key details of changes that include high-level topic (e.g., People and Permissions, Telephony, etc.), action taken (read, view, update, etc.), action details and user executing the action.

Incident management

Potential security incidents detected within or affecting the Genesys Cloud platform are reported to the Genesys Security Incident Response Team (SIRT), who will activate and follow the Genesys Incident Response Plan that includes detailed security incident handling procedures for analysis, containment, eradication and recovery with minimal impact to confidentiality, integrity or availability.

Operational resilience

High availability: Genesys Cloud operates in geographically distributed AWS data centers that are designed to maintain service continuity in the event of a disaster or other incident within a single region. Genesys Cloud services are tolerant of a collective microservice failure, a data center failure or an entire AWS Availability Zone (AZ) failure.

Business continuity: The Genesys Cloud platform is physically separated from the Genesys corporate network environment so that a disruption event involving the corporate environment doesn't impact the availability of the Genesys Cloud services. We also maintain a Business Continuity Plan (BCP) for critical business operations and personnel.

Compliance and attestations

The Genesys Cloud service and facilities meet the rigorous standards and compliance needs of our customers around the world. We demonstrate our commitment through independent third-party audits and the achievement of numerous regulatory and industry certifications.

Global

C5

The cloud computing compliance criteria catalogue (C5) defines a baseline security level for cloud computing. It's used by professional cloud service providers, auditors and cloud customers.

CSA CAIQ

CAIQ is an industry-accepted way to document what security controls exist in our SaaS solutions, providing security control transparency through compliance with the Cloud Controls Matrix.

ISO 27001:2013

ISO 27001:2013 is a globally recognized standard for an information security management system (ISMS). Achieving the certification demonstrates the application of the ISMS principles, as well as the application of ISO 27002:2013 controls to secure and protect organizational data within the scope of the certification.

ISO 27017:2015

ISO 27017:2015 extends the security controls of ISO 27002 to cloud environments. For Genesys Cloud, it's achieved in conjunction with ISO 27001, which involves external verification that the controls are applied appropriately and are managed and sustained.

ISO 27018:2019

ISO 27018:2019 is the globally recognized certification extension to ISO 27001:2013. Achieving the extension certification demonstrates the application of ISO 27002:2013 controls to secure Personally Identifiable Information (PII)/privacy data in the cloud.

PCI DSS

PCI DSS is the globally recognized standard for security policies, technologies and ongoing processes that protect payment systems from breaches and theft of cardholder data.

SOC 1 Type 2

SOC 1 Type 2 is an independent report on management's description of the Genesys Cloud platform and on the suitability of the design and operating effectiveness of controls in accordance with SSAE 18. SOC 1 reports are primarily concerned with controls that are relevant for the financial reporting of customers.

SOC 2 Type 2

SOC 2 Type 2 is an independent report on the description of the Genesys Cloud platform and on the suitability of the design and operating effectiveness of its controls relevant to security, availability and integrity, pursuant to SOC 2 Type 2 examination under ISAE 3000.

SOC 3 Type 2

SOC 3 Type 2 is an independent report on the description of the Genesys Cloud platform and on the suitability of the design and operating effectiveness of its controls relevant to security, availability, and integrity, pursuant to SOC 3 Type 2 examination under ISAE 3402.

Americas

CCPA

The California Consumers Protection Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of California in the United States.

DoD Impact Level 2

The US Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) provides the baseline security requirements used to assess the security posture of a cloud service offering. Genesys Cloud has been granted a Provisional Authorization (PA) for DoD Impact Level 2 (IL2) from the Defense Information Systems Agency (DISA), leveraging the Genesys FedRAMP Moderate Authorization. IL2 is for non-Controlled Unclassified Information (non-CUI), which includes all data cleared for public release, as well as some DoD private unclassified information not designated as CUI or critical mission data that requires some minimal level of access control.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP®) is a government-wide program that promotes the adoption of secure cloud services across the US federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. Genesys Cloud is FedRAMP Authorized at the Moderate Impact Level.

HIPAA

Compliance with the Health Insurance Portability & Accountability Act (HIPAA) demonstrates assurance through effectiveness of security controls that health information is secured and protected.

HITRUST

Health Information Trust Alliance (HITRUST) assures internal and external stakeholders of the current state of information security and compliance, with Genesys Cloud providing greater assurance through the attainment of the externally validated "gold standard" two-year assessment.

LGPD

The Brazilian General Data Protection Law ("LGPD") is Brazil's primary regulation aimed at the protection of personal data. LGPD (Lei Geral de Proteção de Dados) was designed in accordance with the EU's GDPR.

StateRAMP

StateRAMP is a program for US states that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Being StateRAMP Authorized means a cloud system has an established and highly secure environment that has withstood comprehensive audit review before states are authorized to engage the system. Genesys Cloud is StateRAMP Authorized at the Moderate Impact Level.

TX-RAMP

TX-RAMP is the Texas Department of Information Resources (DIR) framework for collecting information about cloud services security posture and assessing responses for compliance with required controls and documentation. TX-RAMP requirements apply to Texas state agencies, institutions of higher education and public community colleges. Genesys Cloud has achieved TX-RAMP Level 2 Certification.

Europe, Middle East and Africa

AgID

The Agency for Digital Italy (Agenzia per l'italia Digitale or AgID) is the "technical agency of the Presidency of the Council of Ministers." AgID's cloud strategy is intended to provide "a qualification path for public and private entities to provide Cloud infrastructures and services to the Public Administration (PA) with high standards of security, efficiency and reliability."

Cyber Essentials Plus

Backed by the UK government and overseen by the National Cyber Security Centre (NCSC), Cyber Essentials Plus is a certification program designed to show an organization has a minimum level of protection in cyber security through annual assessments to maintain certification.

ENS

The National Security Scheme (Esquema Nacional de Seguridad or ENS) applies to the entire Spanish public sector, as well as to suppliers that collaborate with the Administration. ENS offers a common framework of basic principles, requirements and security measures for the adequate protection of information and services. Genesys Cloud was audited by an accredited independent assessor and has achieved ENS High Certification.

GDPR

The General Data Protection Regulation (GDPR) is a data protection law that regulates the use of personal data of EU residents and provides individuals rights to exercise control over their data.

HDS

Introduced by the French governmental agency for health, “Agence du Numérique en Santé” (ANS), the “Hébergeur de Données de Santé (HDS) certification imposes advanced security and privacy requirements on hosting services and cloud providers to ensure that the confidentiality and integrity of sensitive data is adequately protected.

Asia-Pacific

IRAP

Intact Security conducted an audit (known as an assessment) as defined in the Australian Signals Directorate (ASD) Information Security Manual (ISM) and in accordance with the Genesys Cloud SOA. The ISM is developed with the principle of providing Australian government agencies with a baseline of generic risks and controls associated with the storage and handling of security sensitive and classified information.

Disclaimer

Any and all the information provided in this document is provided on an “as is” basis without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose or any warranties regarding workmanlike efforts, lack of negligence or non-infringement. Genesys makes no warranty that the information contained in this document or any tools or services available or offered will be accurate or reliable; or that the quality or features of any products or services described will meet your expectations. The content of the document may include technical inaccuracies or typographical errors. Genesys may make improvements or changes in the products or programs described in this document at any time without notice.

GENESYS™