Genesys Multicloud CX general security overview

11/12/2025

Contents

Provides an overview of Genesys Multicloud CX general security

General security overview

Genesys views security as fundamental baseline for any successful product offering. Genesys Multicloud CX has security built into its solutions at the design and process levels, as an integral part of operations. This program is designed based on industry best practice risk management frameworks realized in precise policies, procedures and standards approved by executive management. The security of the products and the processes to operate by Genesys SaaS Multicloud CX are validated by independent third-party audits as part of our compliance certifications. Details of supported security standards can be found here.

All developers are required to be trained in secure development based on OWASP, SANS 25 and CWE and are not allowed to check in code until such time as this training is completed. Processes and policy are enforced controls upon promotion to production repositories based on scan results and AppSec security review. All product elements are subject to annual audits by a dedicated application security team, which include validation of scanning practices, review of threat models, runtime configuration and internal penetration testing.

Genesys recognizes the great responsibility of being custodians of our customer's precious data. In Genesys SaaS offers all communications over public networks support TLSv1.2 or encryption of equivalent strength. Encryption at rest is leveraged for all persistent customer data storage using AES with 256 bit or higher keys and in many cases at multiple layers (file, datastore, …). And customers may bring their own encryption keys for recordings of their interactions and for data stored for offload from the platform. Logical tenant data segregation is carefully designed for and validated. Additionally, Multicloud CX has built in features that minimize risk of customer sensitive data ending up in any platform logging.

For your users, Multicloud CX can integrate to your directories using SAML2.0 so you can control and monitor your users' access as part of your standard IT platform. The platform has built in role-based access control (RBAC) to make administration easy, and permissions are customizable so you can tune to your business needs. Extensive data is available both via API and through data export so you have full visibility how your services are being used.

The Multicloud CX SaaS offers operate in a geographically dispersed architecture to ensure availability, business continuity and disaster recovery of your services and data. And this platform is protected by best of class security tools, including firewalls, egress proxies, DDoS protection, intrusion detection, anti-malware/endpoint detection and response, VPN, multifactor authentication, secrets vaults, file integrity management, user and entity behavior analytics and vulnerability scanning including container specific scanning with all information from these sources correlated into centralized SIEM with appropriate alerts configured and response plans in place. This infrastructure is operated by certified security experts with years of industry experience with monitoring by a 24/7 SOC. Fully tested and validated incident response procedures are in place in case of need.

Genesys Multicloud CX operates under a comprehensive security program where security foundational from cradle to grave.

Containerization for Azure

Multicloud CX on Azure leverages an evergreen model built on containerization that brings numerous advantages. Containers are built on secured golden base images and are deployed frequently to production avoiding risks of stale content where security vulnerabilities may creep in. Promotion and deployment are managed through infrastructure as code which allows to limit personnel access to production environments compared to traditional architectures. And new containers versions go through multistage promotion through testing environments that allow for strong assurance in Change Management decisions before release to the production environment.