Security Brief

TCN Information Security Brief

Trust is the foundation of any successful relationship. At TCN, we earn the trust of our customers every day by delivering a platform built on availability, integrity and confidentiality.

Founded in 1999, TCN combines a deep understanding of the needs of contact centers with a unique approach to pricing (no contracts, monthly minimums, or maintenance fees) that supports rapid scaling and instant flexibility to changing business needs.

Overview

TCN is an international Software-as-a-Service (SaaS) provider of contact center technologies. TCN's contact center platform, Operator, features a holistic set of easy-to-use, automated agent tools and advanced apps for omnichannel communications, workforce engagement, compliance and data management, integration and automation, intelligence, reporting and analytics, and collaboration and accessibility.

Infrastructure

TCN has partnered with Google to deliver its award-winning cloud-based platform. TCN's Operator platform is a fully containerized (Kubernetes - https://en.wikipedia.org/wiki/Kubernetes) and encrypted service mesh (https://linkerd.io) environment hosted in Google Cloud Platform (GCP) utilizing the Google Kubernetes Engine (GKE). No production services or devices are hosted on TCN premises. Google's data centers are state-of-the art tier 5 facilities (https://www.google.com/about/datacenters/data-security). Access to Google data centers is tightly controlled. Google incorporates multiple layers of physical security to protect data center floors, including biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection. TCN's Systems Engineers access our environments via remote access. Access to TCN's environments utilize strict Identity Access and Management (IAM) policies, requires Multi-factor authentication, uses rotating ephemeral keys, and per cluster certificates over TLS encrypted connections (HTTPS, SSH). TCN's Operator platform is deployed globally in seven GCP Regions, and across multiple Availability Zones within each GCP Region. While Google is ultimately responsible for Service Level Objectives of the infrastructure, in the event of an incident affecting a GCP Region or Availability Zone, TCN and Google will operate in shared responsibility to normalize or restore TCN's cloud-based platform in the affected Region/Zone or an unaffected Region/Zone.

Encryption

By default, all data is encrypted at rest and in transit. Additionally, recording data is encrypted at the file level.

Type	Data Type	Encryption
File Level	Recordings	AES256 using Golang AEAD and GCM cipher modes
At Rest (Disk)	All	AES256 encrypted using the Tink cryptographic library with the FIPS 140-2 validated module BoringCrypto
Transmission	All	Transport Layer Security (TLS) version 1.2 and 1.3 (preferred)
Authentication	Password	Bcrypt Hash & Salt

Data Locality

Data locality is covered in the Google Cloud Platform terms of service (https://cloud.google.com/terms). TCN currently operates seven environments. Data for each TCN environment does not leave the designated GCP Region.

TCN Environment	GCP Region	Physical Location
U.S. and Latin America	us-central1	Council Bluffs, Iowa, U.S.A.
Canada	northamerica-northeast1	Montreal, Quebec, Canada
Austrailia and New Zealand	australia-southeast1	Sydney, New South Wales, Australia
United Kingdom	europe-west2	London, England, United Kingdom
Europe	europe-west3	Frankfurt, Germany, Europe
U.S. East	us-east1	Moncks Corner, South Carolina, U.S.A.
India	asia-south1	Mumbai, Maharashtra, India

Security and Compliance

TCN's commitment to security and compliance remains its first priority. As an integral part of this commitment, TCN incorporates compliance auditing, penetration testing, vulnerability, web application, container image, and secure data transmission scanning into its regular security and compliance activities. TCN utilizes certified auditing firms, Approved Scanning Vendors (ASV), open-source, and proprietary tools to achieve this objective. TCN's security auditing initiatives include:

- Payment Card Industry Data Security Standard (PCI DSS): Security framework and standards designed to ensure that companies that handle credit card information maintain a secure environment.
- Health Insurance Portability and Accountability Act (HIPAA): United States legislation that provides data privacy and security provisions for safeguarding private information.
- System and Organization Controls (SOC) 2: Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.
- International Organization for Standardization (ISO) 27001: International standard for information security. TCN is currently engaged with an accredited ISO certification body (A-LIGN), expected certification completion in Q2 2023.

Google understands security in the cloud. Google's security auditing initiatives include:

- PCI DSS
- SOC 2
- HIPAA
- ISO 27001
- https://cloud.google.com/security/compliance