SECURITY WHITE PAPER

CloudTalk.io, Inc.
150 West 25th Street, RM 403
10001, New York City, New
York United States

August 2022

TABLE OF CONTENTS

1. Our company and products

CloudTalk is the world's leading cloud-based calling software for sales, customer support and ops teams. Since 2014, CloudTalk has been shaping the phone industry with ready-made integrations, advanced user-friendly customization and revolutionary workflow automation options.

CloudTalk is offered as a Software-as-a-Service (SaaS) solution. It is accessible as a desktop app, mobile app (iOS & Android), and Chrome browser (phone.cloudtalk.io).

2. Technology

CloudTalk is a cloud-based software platform that relies on state-of-the-art technology for maximum security and availability. All CloudTalk data is stored in modern safe data centers with 24/7 monitoring.

CloudTalk uses secure data centers of Amazon AWS and Google Cloud Platform in 9 globally distributed data centers with the accessibility of minimum 99.993%. These data centers provide a high level of security all over the world with SOC2 Type II and ISO 27001 certifications, among others. They use multi-level biometrics and other security safeguards to restrict physical access for authorized persons only. The full redundancy of these data centers ensures that your data is safe even in the event of a system failure or a disaster.

CloudTalk employees do not have physical access to Amazon and Google data centers, servers, network equipment, or storage.

More details can be found at https://aws.amazon.com/security

3. Certifications & Compliance

ISO 27001 - CloudTalk is ISO 27001:2013 certified. CloudTalk undergoes regular ISO/IEC 27001 audit conducted by reputable third-party auditors

Penetration testing - CloudTalk undergoes regular penetration testing conducted by an independent, 3rd-party security company. Penetration testing is performed no less than annually. No customer data is exposed to the security company through penetration testing. Outcomes of penetration testing are used to set mitigation and remediation priorities.

4. App security

CloudTalk uses a combination of various security tokens. Communication through our web interface is fully encrypted with the latest TLS version supporting Forward Secrecy.

All data is encrypted during transmissions between the client and the server.

- All passwords are encrypted by an advanced one-way algorithm. Passwords are never stored for internal purposes.
- All phone calls made through the WebRTC protocol are automatically encrypted and those made through the SIP protocol can be encrypted by TLS.
- CloudTalk does not retain information on customer credit cards. All data is directly submitted to our payment processor and our company does not even have access to such information (data is encrypted from the moment the transmission starts).

Encryption

- All data sent to or from CloudTalk is encrypted in transit using 256 bit encryption. Our API and application endpoints are TLS/SSL only and score an “A+” rating on Qualys SSL Labs‘ tests. This means we only use strong cipher suites and have features such as HSTS and Perfect Forward Secrecy fully enabled.

High availability

- Every part of the CloudTalk uses properly-provisioned, redundant servers (e.g., redundant voice infrastructure, multiple load balancers, web servers, replica databases) in the case of failure. As part of regular maintenance, servers are taken out of operation without impacting availability.

Security team

- CloudTalk's infrastructure is constantly monitored and in the event of any threats, our security team is ready to step in 24 hours a day.

SSO

- CloudTalk offers your existing identity provider/SSO solution to be connected. The supported solutions are Google SSO, OneLogin, Okta, Microsoft Azure and Keycloak..

5. Accessibility

CloudTalk's products and processes are designed with the mindset that your data belongs to you. If you ever choose to move to another platform, we will not hold your data hostage.

CloudTalk provides secure API access to customers (except for the "Starter" plan). This means that you are free to use the extensive set of endpoints for more complex actions on your data or to extract any and all data elements in your account. You can find our API reference at https://developers.cloudtalk.io/

5.1 Privacy policy

The privacy of our customers' data is one of CloudTalk's primary considerations. Internal CloudTalk teams (mainly Legal and Security) work together to ensure an effective and consistently implemented privacy policy. Information about our commitment to the privacy of your data is described in greater detail in our Privacy Policy and Data processing agreement.

We would like to point out from the privacy policy that we never sell your personal data to any third parties.

5.2. Data retention

Clear data retention rules are an essential part of minimizing the risk of sensitive data being compromised. By default, CloudTalk will keep your data as long as your account is open and for 6 months after it is closed. After that, the data will automatically cycle out of our daily backups within 1 month. We keep your data to avoid complications if accounts are closed temporarily, due to expired payment methods, or otherwise. If you would like us to permanently delete any data in your account, our customer support engineers will do this for you promptly with our purpose-built internal tools.

For call recordings, it's possible to specify a shorter period, if requested by the customer. E.g. if you would like to purge recordings after 30 days, it's possible to set it up.

6. Authentication

6.1. Login Options

CloudTalk is designed to serve companies of various sizes in any industry. In order to meet these expectations, we have taken care to provide several options for user authentication ranging from the traditional password-based login to Single Sign-on.

6.2. Password

Password Authentication using only a password is the default option to help you get started quickly. It is important to understand that in this case your account's security depends largely on the complexity of your password. Due to this, we have the following password requirements:

- New password must be between 10 and 50 characters long.
- Password must contain 1 small letter, 1 capital letter, 1 number and 1 special character.

User credentials stored by CloudTalk are encrypted with the/a crypt algorithm.

6.3. Google account

If you use a Google account for work, you can conveniently sign up and log in through that, saving you from having to remember a separate password for CloudTalk. If you've enabled two-factor authentication, this will be enforced in addition to the Google login.

6.4. Permission sets

When working with a larger team, there will be occasions when you will want certain users to not perform certain tasks. This could be to reduce the chance of mistakes or to avoid duplication of a user's workload. To allow you to categorize your users and dictate what actions they will be allowed access to, CloudTalk offers 4 type of users with various permissions:

- Admin
- Supervisor
- Agent
- Analyst

7. Vulnerability management & Penetration testing

The CloudTalk security team manages a multi-layered approach to vulnerability scanning, using various well-known tools to ensure comprehensive coverage of our technologies.
To detect and react to the latest vulnerabilities, we execute vulnerability scanning on a regular basis. The scanning is performed particularly against our internal networks and applications but also against corporate infrastructure.

CloudTalk undergoes regular penetration testing conducted by an independent, 3rd-party security company. Penetration testing is performed no less than annually. No customer data is exposed to the security company through penetration testing. Outcomes of penetration testing are used to set mitigation and remediation priorities.

8. Business continuity

Business continuity and disaster recovery plans at CloudTalk are aimed at preventing outages and executing prompt recovery strategies in case the problem is related to accessibility or performance. Outages are averted with the redundancy of telecommunications, systems, and business operations.
Whenever issues affecting the customers arise, CloudTalk prioritizes fast and transparent isolation and resolution of an issue. We publish the identified errors on CloudTalk's status site and update them until they are solved.

9. Back-up strategy

Production data is backed up leveraging multiple online replicas of data for immediate data protection. All production databases have no less than 1 primary (master) and 2 replica (slave) copy of the data live at any given point in time. Replicas are spread to different regions and multiple availability zones.

30 days' worth of backups is kept for any database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary service no less than daily.

Snapshots for Call Data Records are taken and stored on an hourly basis.

For customers who would additionally like to back up their data, CloudTalk provides many ways of making sure you have what you need. Many of the features within your CloudTalk account contain export features, and public APIs can be used to synchronize your data with other systems.

CloudTalk maintains its own continuous monitoring services in order to ensure control and availability of customer data, including:

- Database monitoring
- Application monitoring
- Error reporting and monitoring

For visibility into our availability, we publish status, uptime, and incident reports at https://status.cloudtalk.io

10. Incident management

CloudTalk offers you 24x7x365 coverage and insurance of immediate response to all security and privacy matters. We guarantee the response program to be perceptive and repeatable. It is important to track the issues in advance, set assignments, but also to ease escalation and communication. Redefining incident types is very helpful with this process. Automated processes like notifications of suspicious activity, aberration, privacy issues, customer requests, or supplier alerts are also a great advantage with issue response operations. The first step in incident response is to define information exposure and the potential source of the security issue. Then, we acquaint customers and other involved persons with the issue update via email or phone (in case the email is not sufficient). To resolve the issue in an appropriate way, we secure the regular updates.

11. CloudTalk & GDPR

CloudTalk is committed to privacy, transparency, and high security. From the GDPR perspective, we are committed to complying with EU data protection requirements that became enforceable on May 25, 2018. We have decided to apply the GDPR measures to all clients, including those outside the EU, that are not directly affected by this measure. We believe it will help to increase the security and credibility of all services.