CYTRACOM

RESTECH SOLUTIONS

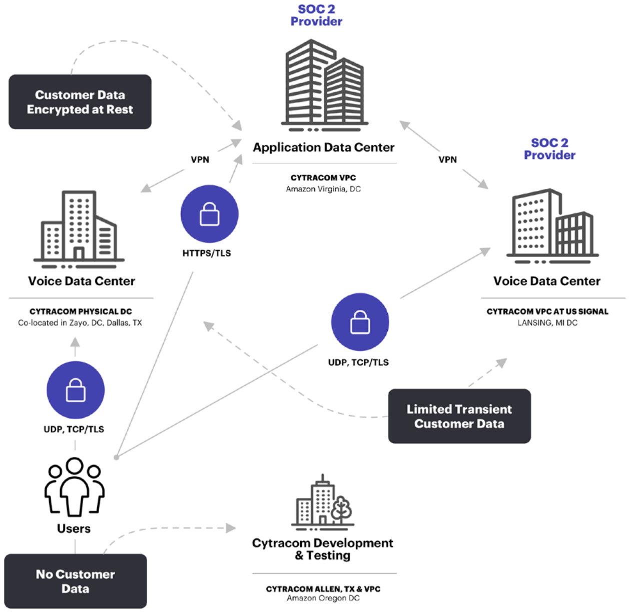
Security Overview

Protecting Your Data & Privacy

Cytracom is focused on infrastructure and application security for our partners and customers.

Data Transport

All of Cytracom's customer data and third-party interactions for essential services are encrypted using TLS v1.2 or above. Web content is hosted in AWS EC2 instances behind AWS and our firewalls with restricted access are only on port 443 for SSL. All port 80 requests are routed to an SSL connection. The primary customer data does not travel outside this data center. The information required to provide the phone service travels to our voice data centers via a secure VPN connection. Cytracom's voice data centers do not have any web-based access or any direct user access to any data. Our customers choose to connect their phones either via UDP generally, or via TCP/TLS when transport encryption is priority over performance.



Data Storage

All of Cytracom's primary and sensitive data are stored in our application data center within AWS encrypted at rest. Before a request gets to the data in the encrypted storage, it goes through several layers of checks and balances via isolated containers. An invalid request is stopped several layers ahead of your data. Cytracom uses cloud-based collaboration tools and store all our communications and contact information in Google Application Suite and Zendesk.

Protecting Your Data & Privacy

Data Retention

Cytracom stores call detail records (CDRs) for up to 5 years or to an extent required by the law in our application data center. If a customer chooses to selectively record calls, the retention of these will follow the criteria specified by the customer. Unless a customer chooses to store voicemails, all voicemails are typically removed after it's emailed to the recipient. Voicemail retention also follows the criteria specified by the customer.

Application Security

All of Cytracom's call control applications are built from ground-up using a programming language known as Erlang. This is a very niche language with limited and mature libraries. We strategically chose this language for security and reliability. In the case that the data within the application gets corrupted, the application will reboot that segment of the application without impacting the overall function. Cytracom doesn't use third-party, contract or offshore resources to develop applications. We design and build all our applications in Allen, TX. This ensures that our applications are secure and protect your data.

Infrastructure Security

At Cytracom we only use Linux in our infrastructure and we limit this to Ubuntu LTS, Debian LTS and VMWare Photon. We also run all our applications other than the base voice service in Docker containers with low privileges isolating each other. Cytracom has explicitly locked down our firewalls to only allow protocols absolutely necessary for our voice services such as Port 5060, 5061 and 5062 for SIP and on demand UDP ports with very limited range for RTP/RTSP protocol.

Endpoint Security

Though we typically remote access all our operational and development environments from portable devices, we also encrypt all our Windows and Mac portable devices to mitigate situations where a device can be lost or stolen. We ensure that these devices have up-to-date threat management software and anti-virus software.

Security Testing

The source code that Cytracom produces and other third-party libraries are scanned regularly to make sure they do not contain vulnerable components. We use scanners at the repository level to automate scanning and generate alerts if a vulnerability is found. We also conduct periodic pen-testing.

Protecting Your Data & Privacy

Privacy Policy

Cytracom has a strict privacy policy that ensures your data remains private even from our employees. Not only does Cytracom have role-based security protecting call-recording and voicemail data from unauthorized personnel within customer organizations; we also extend that restriction to our support staff. For example, our support techs can see that you have a call recording, but they can't hear the audio. Cytracom also provides limited access to a reseller or MSP who sells and installs a customer phone system. Unless the customer specifically allows the reseller or MSP access, they are also prevented from accessing any data outside the basic PBX setup.

Restricted Access

Only a few employees at Cytracom have direct access to the production environment. Even within IT operations other than Chief Security Officer (CSO) all other engineers have partitioned access. The CSO can provide access to an engineer when needed and remove that access when not needed. Our developers have no access to the production environment or data, and we anonymize data before we copy some limited set to the testing environment to reproduce issues.

Third-Party Services

Cytracom integrates with best-in-class third-party providers to deliver key services to our customers. This includes voice transcription using Google Cloud Platform (GCP) and payment processing using Authorize. Net and Dwolla. We use Authorize.Net for credit card processing and Dwolla for ACH processing. Cytracom does not store any Credit Card or ACH information, only an encrypted reference to these services for recurrent payments.

Two-Factor authentication

At Cytracom we have our own single sign-on service (SSO) protected by 2FA using TOTP to access our web portal and other applications. Due to the SSO we only maintain a single password per user, salted and encrypted to the highest effort levels.

SSAE SOC 2 Compliance

Cytracom is currently going through the process of getting our environment SOC 2 Type 2 compliance, and a report will be ready during Q3, 2021.

CYTRACOM

877.411.2987 | www.cytracom.com |