CAPTURI SERVICE DESCRIPTION, SETUP AND SECURITY MEASURES BASED ON FAQ

TECHNOLOGY

How is the Capturi platform build?

Web Frontend

The web app is build with modern web technology, primarily React.

Backend

The backend serves as an API for the frontend. The API(s) is build on dotnet core 3.1 and by use of Mongo DB as storage.

Our ASR (Automated Speech Recognition) is build in Python and Java.

Mobile

We only have a POC of the iOS app at the moment. The strategy going forward is to build mobile apps in native languages. By use of native language you get a much better user experience and performance together with the benefits of using the same API(s) as the web app.

Integrations / API

By use of our API you can connect a wide range of different systems to Capturi.

DATA STORAGE

Where are Capturi's data centers?

Capturi stores customer data on datacenters delivered by Amazon Web Services (AWS) which we deem to be a market leading secure data storage and hosting provider.

All data is located in EU, including backups etc. The specific AWS region our data is contractually stored in is EU (Ireland) eu-west-1.

You can see more about the datacenter's physical security, full list of security certificates, and other details by following these links:

Amazon (AWS) https://aws.amazon.com/compliance/data-center/data-centers/ and https://aws.amazon.com/compliance/programs/

DATA RETENTION AND DELETION

How is customer data backed up?

All client audio files are stored in blobs that are replicated to at least 3 availability zones (redundant and separate power, networking and connectivity) within our datacenter region.

All client data is fully backed up on hourly/daily/weekly/monthly basis within the same datacenter region. Backups are kept for up to a year based on the backup frequency (Monthly backups are kept 12 months, daily 7 days, weekly 4 weeks, hourly 2 days).

Can Capturi delete customer data?

Generally all data, including user data, added by the customer to the Capturi platform can be deleted by the customer's registered users.

Specific data deletion request and specific data on users can be made with written request to Capturi.

1. Upon a request of deletion of data, the delete process is:
2. The customer provides a delete request to our support.
3. We will make a verification with account owner to ensure that we understand the need for deletion.
4. We will make a delete script and verify the output with account owner.
5. Excecution of delete script

The delete script will be saved for 21 days to ensure that we can delete the data again, if a datarecovery has occured in the period.

Does Capturi keep customer information after termination?

Capturi allows customers to export their raw data at any time in the industry-standards like JSON for the meta data and mp3 for audio format. Additionally, customer data can be deleted upon request at termination as per above. In the absence of such a request prior to termination, customer data will be deleted in accordance with Capturi's internal data retention policies.

DATA SECURITY AND MANAGEMENT

Does Capturi keep one customer's data separate from other customer data?

A customer's data is stored in document database systems which house data belonging to other customers, but our architecture and logical controls (token, key and secret) separates one user's data from other users data.

Does Capturi support single sign-on and multifactor authentication?

Our product supports single sign-on and provides authentication options through different providers. We always recommend use of the multi factor authentication.

ENCRYPTION AND PASSWORD MANAGEMENT

Data in transit - Does Capturi encrypt the communication?

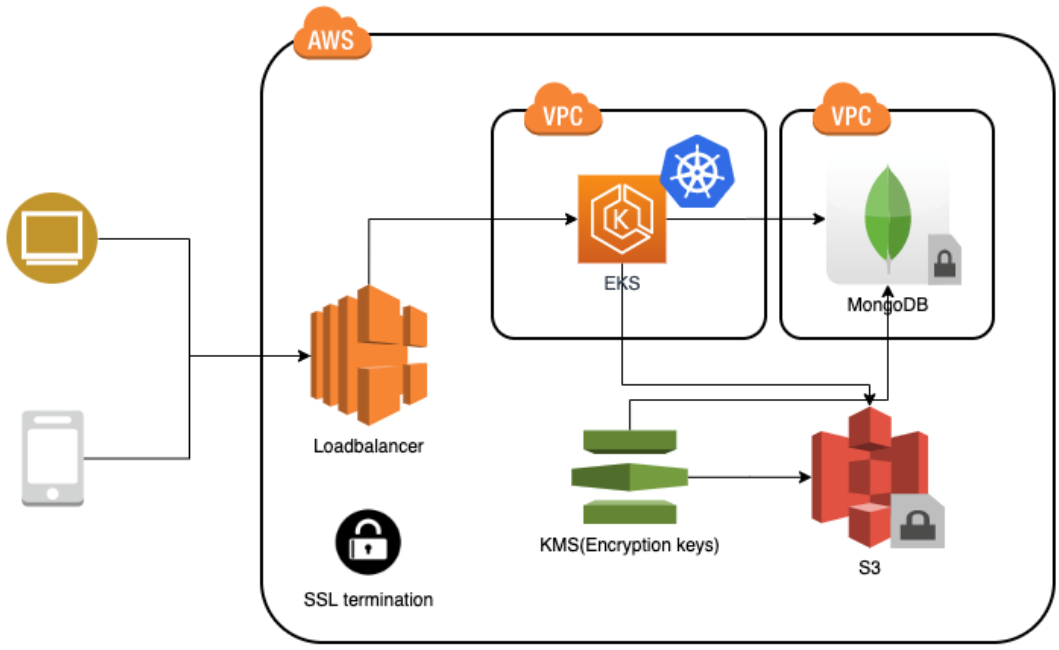
All internet communication to Capturi is encrypted using https (TLS 1.2). Unencrypted traffic (http) is redirected to https.

Data in rest - Does Capturi encrypt customer data?

We encrypt customers data by default and logically isolate customer data. Both blob storage and MongoDB is encrypted using AWS KMS.

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

https://docs.atlas.mongodb.com/security-aws-kms/#security-aws-kms



Are user's passwords encrypted?

By providing several login providers (Microsoft Office 365, Google) to our customers we do not have the need for storing the user's passwords. The selected login providers provides additional security like MFA.

What are Capturi's corporate password requirements?

For accessing the production environment, we always use Multi Factor Authentication (Software MFA - Google Authenticator). With regards to the password policy specifically, they are set as follows: (a) passwords must be a minimum of 8 characters; (b) they must contain some lower case letters, and they cannot contain part of the username; and (c) users can not reuse their passwords.

Access to personal data and the production environment

For accessing the production environment, including servers, use of Multi Factor Authentication (Software MFA - Google Authenticator) is a requirement. Capturi restricts such access to selected employees who has a work related purpose to access the systems and data, and Capturi log all employee access to systems that contain personal data. All access to the production environment will be logged. Management continuously assess whether employees with access have a work related need for access.

Monitoring

Does Capturi monitor the platform?

We are constantly logging all kind of activity in the platform, and are monitoring availability, response time, error rate, server load to ensure that the platform is in a healthy state.

Real time dashboards are always present for our developers for a real time overview of all our services. Any access to customers data requires prior consent from the customer to access the specific data.

Audit logging

Does Capturi log actions?

The audit log contains authentication information about token usage. Since we are using external login providers we do not have a real login session, but rely on authentication from the login provider. We are logging all successful sessions.

Logging of expired tokes, modified tokens and disabled tokens are monitored constantly.

HR/CORPORATE POLICIES

Does Capturi run background checks on its employees?

We run background checks on all incoming employees, or contractors who will be working in any Capturi office, before starting work at the Company. Additionally, all employees and contractors sign confidentiality agreements to protect customer information.

Does Capturi subcontract any of its services?

Capturi uses third-party vendors to provide the services, namely AWS. Capturi additionally uses vendors to monitor the usage and performance of the Applications after they have been vetted and signed appropriate contractual protections, but such vendors will not have access to added customer's data, but only anonymized and aggregated log data on users i.e. time stamps, platform usage etc.

How does Capturi select its subcontractors?

Capturi has a vendor assessment policy that includes security team review of the vendor use case, their security posture, and their ability to access personal information. The legal team additionally requires privacy and security provisions in the contract where necessary to protect customer information.

GDPR

Does Capturi process personal information?

Capturi's customers are in full control of what information they add to our platform and contractually bound to ensure legality and legal basis for adding the information to our platform. This information may include personal information at the choice of the customer and Capturi's handling and processing of such data will be in accordance with the regulation set out in the data processing agreement entered into with the customer either directly or indirectly.

Is Capturi a data controller or processor?

When customers add data to the Capturi platform, Capturi is the data processor or subdataprocessor, as defined in the GDPR, for processing required for the purpose of providing the agreed services directly to the customer or through a partner. The end customer is always the data controller, as defined in the GDPR.

Does Capturi comply with GDPR?

Capturi is committed to complying with, and enabling our customers to comply with, GDPR.

AUDITS

Does Capturi have security certifications?

Capturi stores customer data with our hosting provider, Amazon AWS, who has annual audits for the following standards: ISAE 3402 Type II: SOC 1; SOC 2; SOC 3 public audit report; ISO 27001, one of the most widely recognized, internationally accepted independent security standards; ISO 27017, Cloud Security. This is an international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services; ISO 27018, Cloud Privacy.

Does Capturi conduct regular internal and external audits?

Capturi has strong internal procedures to ensure compliance with IT security and GDPR procedures, and welcome audit requests from its customers. Capturi will, once the time is right, work on getting ISAE-3000 statement from an independent auditor to further evidence Capturi's commitment to comply with GDPR.

THREAT AND VULNERABILITY MANAGEMENT

How does Capturi approach patching of software?

Select employees is notified when updates are available to the production servers (New EKS AMI's and versions). We check for updates to internal software in our Kubernetes cluster on a regular basis. (dns, proxy, monitoring, ingress, etc).

Does Capturi have anti-malware programs installed?

All docker images is scanned for vulnerabilities when they are pushed to our container registry (AWS ECR).

Does Capturi do penetration testing?

We engage respected ethnical hackers on an annual basis for manual penetration tests.

How does account management work on Capturi?

Authorized Capturi employees, such as our support staff, have access to customer data for the purposes of supporting and operating the service. Access will, however, only be made on the request from a customer and subject to their prior consent to access. Employees are trained on appropriate access, and all access is monitored for inappropriate use.