WHITEPAPER //
SECURITY

captionhub

OVERVIEW

Your content is critically important. CaptionHub has been designed to be as secure as possible, and we do all we can to ensure that your data is only accessible by those you give access to.

This document outlines some of the steps we take to secure your data.

Unless we specify otherwise, this document relates to our cloud service on AWS. Please contact us with specific deployment requirements.

Document last modified: 24th September 2020

Notices

This document is provided for informational purposes only. It represents CaptionHub's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of CaptionHub's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from CaptionHub, its affiliates, suppliers or licensors. The responsibilities and liabilities of CaptionHub to its customers are controlled by CaptionHub agreements, and this document is not part of, nor does it modify, any agreement between CaptionHub and its customers.

CONTENTS

RISK MANAGEMENT AND SECURITY

LEADERSHIP COMMITMENT

CaptionHub's management team leads the organisation's commitment to a highly secure operating environment, information environment and platform. Security objectives have been established according to our strategic objectives - a Security Working Group chaired by our CEO oversees information risk and security management. A systematic review of internal security performance is conducted through an internal and external audit programme, and through a system of continual improvement compliant with international security standards including ISO27001.

CONTINUAL IMPROVEMENT

CaptionHub has a system and culture of continual improvement in relation to its approach to risk and security management. We continually improve the effectiveness of our internal security procedures, documentation and systems so that we can offer the highest standards in enterprise security. The entire team is encouraged to and does contribute ideas and improvements to risk and security management. In line with ISO27001, risk planning and documentation, incident management and non-conformance logging are all carried out in our business as usual activities. Please contact us if you require further information on any aspect of this.

RISK MANAGEMENT AND SECURITY

RISK MANAGEMENT

Risk and security management occurs at every level of the organisation. Our systematic approach to risk management includes management planning to align risks to achievement of objectives, information and operational continuity management and assessment of risk of changes via a documented change control process. Our Risk Management Framework (RMF) provides definitive information on the measures used to manage cybersecurity and information related risk. Protecting data and the systems that collect, process, and maintain data is of critical importance to you and us. Consequently, our security ensures we have controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of your data.

CONTINUAL IMPROVEMENT

To ensure that CaptionHub continually operates in accordance with its own security and risk management policies, procedures and external requirements in relation to information security, CaptionHub has a comprehensive review system spanning three levels. This includes a structured regular management review of conformity to management procedures and policies; an internal audit review across all security standards, and; an external audit against our information security management system and a technical (penetration) audit of the application.

APPLICATION SECURITY

ASSESSMENT

CaptionHub has been designed for a secure environment from its inception. We regularly carry out the following:

- Application vulnerability scan – we use Detectify to scan our systems every week, using the latest attack vectors
- Application vulnerability threat assessments (on an ongoing basis)
- Network vulnerability threat assessments (on an ongoing basis)
- Penetration testing and code review (at least annually, or after a major architectural change)
- Security control framework review and testing (annually)

ENCRYPTION

- Traffic to and from the browser is encrypted via SSL/TLS (TLS 1.2 with SHA256 certificate).
- Data is encrypted at-rest, using 256bit encryption via Amazon's SSE-S3.

AUTHENTICATION

We use Auth0 to manage authentication, which enables multi-factor authentication, SSO, password strength management, and so on. Custom integration with your own authentication schemes is available for our on-premise customers.

BREACHED PASSWORD DETECTION

Via Auth0, CaptionHub protects and notifies users if and when their credentials are leaked by a data breach of a third party. CaptionHub prevents access until the user has reset their password.

ESSENTIAL SECURITY FEATURES

- By default, a new user for CaptionHub has no access – permission needs to be explicit, and given for each and every project.
- CaptionHub produces an audit trail for logged in users.
- Expiring URLs mean that it's difficult to download linked media, even if access is granted.
- Logged in user's email address superimposed over video, making screen captures traceable
- Enterprise customers benefit from additional security measures, including
  - IP whitelisting
  - 2 factor authentication
  - SSO / custom authentication
  - Watermarking encoded media

CERTIFICATION

- CaptionHub has full ISO27001:2013 certification
- CaptionHub has achieved Cyber Essentials certifcation.
- CaptionHub has been FACT (Federation Against Copyright Theft) certified.

CODE TESTING

All code at CaptionHub is QA'd before deployment, and a security analysis is an explicit part of that process. We also automatically test all code for security vulnerabilities before release, using static analysis.

THREAT DETECTION

We scan our network and systems for vulnerabilities on a nightly basis. Part of these scans and countermeasures include RKHunter, ClamAV and AIDE. Virus signatures are updated on a daily basis, and the applications themselves are regularly kept up to date.

PERSONNEL

Potential CaptionHub employees undergo an in-depth interview and screening process before employment. Our contracts contain dedicated Information Security clauses, alongside extensive non-disclosure obligations. The on-boarding process includes training, and we operate under the least access principle. As of this document's last revision, seven CaptionHub employees have access to customer data; front line support staff do not, unless explicitly given access by our customers. If a CaptionHub employee's contract is terminated, then access to all systems is revoked in a methodical way.

THIRD PARTY ACCESS

Depending on how CaptionHub is configured and used, you may choose to share your data with third parties. Auto-transcription and machine translation are two examples of this, where CaptionHub uses third parties in order to deliver aspects of our service. Your data is only shared following an explicit action from you, and we have strict contracts in place with all third party providers, with extensive non-disclosure clauses. Please refer

to our Privacy Policy, or contact support@captionhub.com for more details.

DEPLOYMENT

- Servers do not use passwords and require 4096 bit RSA keys to provide access to the box via a bastion server. All keys are unique to individual administrators or service accounts and are not shared.
- Network level firewalls prevent unauthorised traffic from reaching servers in the data centre.

CONTINUITY

HIGH AVAILABILITY

CaptionHub is configured in a High Availability pattern, with no single point of failure. We use infrastructure-as-code to seamlessly scale out services, as required.

BACKUPS

We take daily backups of our database to Amazon S3. We don't back up video data, but we do back up caption data/work so that it can be restored in due course. Incidentally, S3 redundantly stores data across multiple devices and facilities. Video data is also stored on S3, which has a durability rating of 99.999999999%.

DATA CENTRE

For a cloud install, CaptionHub typically hosts our applications and your data with Amazon Web Services (AWS), an industry leader providing highly scalable, secure cloud platform computing platform. Here are some resources from AWS with additional context:

Overview of AWS Cloud Security
AWS Security Processes
AWS Compliance

PHYSICAL SECURITY

AWS has state of the art data centres where physical access is strictly controlled by professional security staff using a combination of video surveillance, intrusion detection systems, multiple sets of two-factor authentication and other electronic means. Only authorised personnel with legitimate business needs are granted access to the data centres. All physical access to data centres by AWS employees is logged and audited routinely and all visitors require ID and are escorted by authorised staff.

AWS maintains and continues to enhance their SOC reports, certifications, including SOC, PCI, ISO and many more. Additional details are maintained on the AWS Compliance section of their website.

BUSINESS CONTINUITY MANAGEMENT

Amazon's infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal

customer impact. Data centre Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

ENVIRONMENTAL SECURITY

- Every data centre has automatic fire detection and suppression equipment.
- They have fully redundant electrical power systems that are maintainable without impact to operations 24x7 and have UPS and back-up generators in case of electrical failure for critical and essential loads.
- Climate and temperature are precisely controlled by personnel and systems to ensure optimal performance of servers and other hardware.
- All systems and equipment are monitored and receive preventative maintenance to maintain continued operability of equipment.

FAQ

Can I install my own instance of CaptionHub behind my firewall?
Yes. For our Enterprise customers, CaptionHub can be deployed in a variety of ways. Please contact us for more details.

Does my data exist alongside other users?
It depends on your install. For our multi-tenant customers, it does. CaptionHub is extremely well tested to ensure that users don't see each other's data, but if you require absolute separation, then we'd recommend you opt for our Single Tenant or On Premise installation options.

Who can see my information?
Access to data is limited to CaptionHub account administrators and developers. From time to time, CaptionHub also employs third party developers, who are strictly contractually bound regarding any confidential information.

Can you produce an audit trail which logs who has accessed what?
By default a user can't see anything in CaptionHub, they have to be manually given access to a project before they can view it. We track user login times and IP address, and we log various forms of activity: handover, download, assignment, etc.

HELP

Please see our KnowledgeBase at captionhub.zendesk.com

Should you have any support questions, you can email us at support@captionhub.com