super.AI

AI FOR EVERYONE

Data Security Whitepaper

How super.AI implements security measures and handles customer data.

security@super.ai

Table of Contents

Table of Contents 1

Introduction 3

1 People Security 4
- Role Based Access 4
- Authentication Policies 4
  - Employee Accounts 4
  - Training 4
  - Customer Accounts 4
- Labelers 5
  - Policies 5
  - Training 5
  - Data 5

2 Data Security 5
- Data Protection by Design 5
  - Encryption in Transit 6
  - Encryption at Rest 6
  - Personal Data Collection 6
  - Testing 6
  - Penetration Testing 6
- Data Permissions 7
- Data Deletion 7

3 Infrastructure and Network Security 7
- Data Centers 7
- Physical Security 7
- Distributed Denial-of-Service (DDoS) Prevention 7
- Security Compliance 7
- Regulatory Compliance 8
- Infrastructure Provider 8
- EU General Data Protection Regulation (GDPR) 8

4 Privacy Rights 8
- Right of Access 8
- Right to Erasure 8
- Stop Processing Data 8
- Data Portability 9

Introduction

Super.AI operates a platform to enable AI to be effectively used in the real world. Our customers trust us with their most sensitive data, therefore, security is a core functional requirement to protect their information from accidental or deliberate theft, leakage, integrity compromise, and deletion.

Information security policies and standards are regularly reviewed and adapted by Super.AI's senior engineering leadership to continuously raise the bar. Changes are approved by the executive management team. All super.AI employees are required to read and keep up to date with the policies. In addition, mechanisms – such as training and monitoring – are implemented throughout the organisation to ensure policies are applied.

1 People Security

Super.AI's employees are fundamental to provide a secure and reliable service to our customers. Below are the core principles that we apply.

Role Based Access

We apply a strict need to know principle when it comes to the access to resources. Employees only have access to resources that are required to conduct their duties. That is, access to operational applications, environments and data is strictly limited to an employee's role. E.g. an employee in Team Alpha can't access the resources of Team Gamma.

Authentication Policies

We apply authentication policies according to industry standards. Both for employee and customer accounts:

Employee Accounts

- We use 1password[1] to generate a random, unique password for each service
- Passwords are rotated regularly
- It is not allowed to share credentials
- We use two-factor authentication when available

Training

An essential part of the onboarding process for new Super.AI employees is a module on our security policies and standards. In addition, we conduct regular training and give updates on security protocols to all employees. Employees who have access to personal data and non-technical employees receive extra training.

Amongst other things the training covers the following topics: email security, passwords, two-factor authentication, device encryption, and use of Virtual Private Networks (VPN).

Customer Accounts

For customer passwords we use Amazon Cognito[2] and follow their recommendations for secure passwords (8 characters length, at least 1 number, at least 1 lowercase letter).

[1] 1password: https://1password.com/
[2] Amazon Cognito: https://aws.amazon.com/cognito/

Labelers

Policies

All labelers must agree to adhere to the terms and conditions and privacy policies found at https://crowd-hero.super.ai/eula and at https://crowd-hero.super.ai/privacy.

Training

After agreeing to the terms and conditions and completing sign up, labelers must complete training before seeing any customer data. Access to customer workloads is given based on qualification and can be revoked at any given point in time.

Monitoring

Labeler performance is monitored and a fraud detection system is in place to prevent and detect malicious behavior.

Data

The source of the data is not known to the labelers (customer information is not shown unless the customer includes it in the job data themselves) and data is not stored locally on their machines (it is only displayed to them).

If required, at additional cost, labelers can be located in a secure facility on company owned equipment with no personal electronics allowed.

2 Data Security

Super.AI's product teams consider security as the number one priority when designing, building, deploying and monitoring our services. Whenever we identify a risk, everything else is put on hold until it is resolved.

Below are core principles we apply across our platform.

Data Protection by Design

Super.AI follows the principle of data protection by design and by default. That is, implementing appropriate technical and organizational measures to protect data.

Encryption in Transit

Super.AI is built in a microservices architecture fashion. All network traffic between services is encrypted. SSL/TLS is enforced for all communication with Super.AI APIs (using Amazon API Gateway[3]). We use encryption or pseudonymization whenever feasible.

Encryption at Rest

All customer data is encrypted at rest. Technologies we use include Amazon ECR[4], Amazon S3[5] and Amazon RDS[6].

Personal Data Collection

We limit the amount of data we collect to those data points that are essential to operate our business. Data that is no longer needed is deleted.

Testing

We apply a test driven development approach. For every change we apply a two-man rule. Our Continuous Deployment pipeline ensures that changes pass multiple gates before they are deployed to production.

Monitoring

Super.AI's services are continuously monitored and relevant thresholds are set to alarm about out-of-band performance. Dedicated employees are monitoring the system in an on-call rotation. We understand that data breaches need to be reported to EU authorities within 72 hours. In addition, we understand that we are required to communicate data breaches to data subjects unless the breach is unlikely to put them at risk (for instance, if the stolen data is encrypted)

Data Permissions

Customer data is stored in dedicated, encrypted S3 buckets, created using the customer's private API key. Customers can invalidate their API key at any given point in time and revoke the access to their data.

[3] Amazon API Gateway: https://aws.amazon.com/api-gateway/faqs/
[4] Amazon ECR: https://aws.amazon.com/ecr/features/
[5] Amazon S3: https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket-encryption.html
[6] Amazon RDS: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

Data Deletion

Customer data is deleted 90 days after contract termination, unless otherwise requested by Customer.

3 Infrastructure and Network Security

Super.AI's platform is built on top of the Amazon Web Services (AWS) infrastructure to provide a secure, reliable and scalable service.

Data Centers

Super.AI's software stack is currently deployed in the AWS US-East (Northern Virginia) Region[7]. The environments leverage multiple availability zones to mitigate the risk of failure.

Physical Security

Super.AI uses AWS infrastructure for all production systems.

For detailed information on Physical Data Security please review the AWS Security Whitepaper (page 10 et seqq.):
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Distributed Denial-of-Service (DDoS) Prevention

The Super.AI platform leverages best practices to prevent and mitigate the risk of a DDoS attack, both on a network and application level.

Security Compliance

Super.AI commits to ensure its services meet regulatory and security standards.

Regulatory Compliance

Super.AI complies with applicable legal, industry, and regulatory requirements as well as industry best practices.

[7] US East Region: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2

Infrastructure Provider

The Super.AI platform runs on AWS infrastructure, which is highly scalable, reliable and secure.

AWS is compliant with global and geographical specific programs and policies, such as SOC, ISO 27001, PCI DSS, and GDPR: https://aws.amazon.com/compliance/programs/

4 Privacy Rights

Right of Access

Super.AI offers data subjects to get information about our data processing activities, including the data we have about them and the purpose for using it. Please contact security@super.ai

Right to Erasure

Customers have the right to ask to delete all the personal data we have about them (unless we are required to keep them to comply with a legal obligation). Requests are typically honored within a month. Please contact security@super.ai

Stop Processing Data

Customers can request to restrict or stop processing of their data. Requests are honored typically within a month. Please contact security@super.ai

Data Portability

Customers can request to get their personal data in a commonly readable format. Requests are processed typically within a month. Please contact security@super.ai

---

If you have further questions please contact our security team: security@super.ai

SUPER.AI INC