WEDGE SECURITY OVERVIEW

March 24, 2022

Wedge Security Overview

Introduction

As a cloud software company, Wedge, we recognize the importance of excellent security practices. While we are a small team, we strive to provide world class platform security. We understand that trust is earned and we are committed to earning yours.

Wedge uses a defense-in-depth approach providing layers of protection throughout our organization. We're passionate about implementing new practices and continuously refining our existing ones.

This document covers our security practices and policies. If you are interested in the data we collect and store, please see our privacy policy.

If you have any concerns or questions, please reach out to security@wedgehr.com.

General Practices

- Access to infrastructure, code, and third-party services are protected with two-factor authentication.
- All passwords are randomly generated with a minimum of 32 characters, and are never re-used.
- We use an automatic vulnerability detection service on all of our code and dependencies, and move quickly to patch issues as they are found.
- Production data is never copied outside of the production environment.
- Access to production data is tightly restricted on a must-need basis.

Personal

Our team members and contractors sign a comprehensive NDA and are trained on industry best practices for security.

Wedge Security Overview

Encryption

- All data is encrypted in transit and at rest.
- Traffic to our API is protected with TLS 1.2 via short-lived certificates provided by Let's Encrypt.
- Traffic to our CDNs are protected with TLS 1.2 or 1.3 certificates which can be reissued on demand.
- Firewalls are tightly configured to allow only necessary traffic.
- Encryption keys are regularly rotated.

Data Storage

We consider data to be one of two types: Media or State. For example, an uploaded video's media content is considered as Media, while metadata about the video is considered State.

Media data is stored in Cloud storage buckets residing in Amazon Web Services S3 and Google Cloud Storage. These facilities are accredited under ISO 27001 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II).

State data is stored on our infrastructure in a colocation facility located in Detroit, MI. We are planning a migration of all State data to Google Cloud Platform. Our colocation facility carries SOC 2/Type 2, HIPAA, PCI-DSS, SSAE-16 certifications.

FAQs

Q: How does the Public Share Link work for a wedge?
A: When enabled on a job, the public share link allows a Wedge to be viewed publicly regardless of authentication. Notes, ratings and other collaboration functionality is only available to authenticated users with access to the Wedge.

Q: Who can access my data?
A: Access to customer data is tightly controlled on a must-need basis, and contains tight auditing records.