Benchling

Security Overview

Benchling's commitment to data security is central to our company. Our success as a product and a company depends on earning and keeping your trust, and we take that very seriously. We know that trust starts with confidence that your company's data is safe with us.

› INFRASTRUCTURE AND HOSTING

Amazon Web Services allow for quick iteration on well-tested systems

Deploying and hosting on Amazon Web Services (AWS) allows Benchling to build on top of well-tested, secure systems, iterate quickly to resolve any issues, and automate configuration and detection of problems. We have an active working relationship with AWS, detailed **here**.

Since Benchling is responsible for running and maintaining servers on AWS, the latest bug fixes and security patches are rolled out without requiring any work from your side.

You can read about how seriously AWS takes security on the **AWS website**. The list of AWS certifications, including ISO 27001 and SOC reports 1, 2, and 3, is available **here**.

› NETWORK SECURITY

AWS virtual networking limits access to production systems

Benchling uses AWS virtual networking technology to create private networks shielded from the public Internet. Access to production systems is always limited to approved networks. Multiple layers of firewalls are applied to allow whitelisted traffic, and network and firewall configurations are reviewed for security on an ongoing basis.

› DATA ENCRYPTION

SSL connections and customer-specific keys ensure effective encryption

Customer data transferred, processed, and stored on Benchling is always encrypted using industry best practices. All data sent over the Internet to Benchling's servers are encrypted over TLS/SSL connections. Data stored in Benchling are encrypted at rest using AES-256 encryption.

> AVAILABILITY AND BACKUP

Files and databases are backed up with extremely high durability

Customer data is at minimal risk of loss thanks to our high-redundancy data storage practices. Benchling divides data into raw files (images and other data uploaded by users) and structured data. Raw files are stored in Amazon S3, which is designed for 99.999999999% durability over a given year: https://aws.amazon.com/s3/faqs/. Older versions of files are retained for 90 days.

Structured data is stored in a Postgres database configured with synchronous replication to a backup. In the event of a database failure, the backup can be switched to with only a few seconds of downtime and a few seconds of data loss. Daily backups of the Postgres database are stored for 35 days and allow for granular data restoration on the level of minutes. Weekly backups are stored for at least 1 year. Backups are replicated geographically for higher redundancy.

> EXTERNAL SECURITY AUDITS

Annual tests of Benchling ensure up-to-date security

We ensure that Benching's practices are up-to-date with current standards and are insusceptible to the latest vulnerabilities identified by security professionals. Third party experts perform rigorous annual grey-box penetration tests of Benchling.

> AUTHENTICATION

Seamless integration with your authentication system

Benchling allows customers to maintain their existing authentication policies so that managing, provisioning, or suspending users is just as easy as ever. By integrating with your existing SAML or Google SSO setup, users can sign in with a single login, and you get all the benefits of your existing setup, including any two-factor authentication and password policies.

> COMPLIANCE

Our products ensure strict compliance to regulatory standards

Our product offerings are designed for regulatory compliance with FDA 21 CFR Part 11 through comprehensive audit trails, electronic signatures, and electronic records support. Our security practices comply with FIPS 200, and our security program aligns with ISO 27001. Additionally, we work with customers to develop SOPs for their usage of Benchling to optimize adherence to recognized standards.

> TEAM

Benchling is built by top Silicon Valley engineers

Benchling hires leading Silicon Valley software engineers. Our team hails from technology leaders such as Google, Palantir, and Twitter, as well as MIT, Yale, and Carnegie Mellon. Our engineers architected Benchling based on best practices in the technology industry, and we work constantly to improve and understand new risks and trends in data security.

More Information

We invite your questions and concerns about data security and privacy. We feel confident we can ensure that Benchling meets your company's workflow and security needs. Please contact us at *support@benchling.com*.