Security and Privacy at Benchling

Security White Paper

Table of Contents

Executive Summary

Benchling provides cloud-native software solutions for life sciences research and development (R&D). These products are trusted by hundreds of global companies that operate in highly regulated industries, including biopharmaceuticals, vaccines, agricultural products, and industrial biotechnology. Customers utilize Benchling's systems to securely store and process critical data pertaining to the design and development of advanced life science products. Because Benchling considers its commitment to protecting customer data as central to its mission, the company employs the most advanced security and privacy measures for data protection.

The intended audience for this document includes security, quality, compliance, and information technology (IT) professionals, as well as R&D leaders, who wish to learn more about Benchling's security posture; including details on technical, operational, and organizational controls. It will help customers understand primary considerations in all the following areas:

Product Security

Benchling has designed and built security into its agile software development life cycle by automating security checks in the development pipeline, placing security champions on scrum teams, and training every developer on secure coding. Benchling's products have controls in place for identity and access management, data protection, and backup.

Operational Security

Benchling maintains an active posture in regard to threat detection, incident management, and disaster recovery and business continuity plans.

Organizational Security

Benchling's dedicated security and privacy programs are externally audited annually. The company maintains an International Organization for Standardization (ISO) 27001 certification, as well as a Privacy Shield certification. All Benchling's operations comply with the Global Data Protection Regulation (GDPR) as well as the California Consumer Privacy Act (CCPA). In addition, Benchling aligns its security program and capabilities with the Cloud Computer Compliance Controls Catalogue (C5), National Cyber Security Center (NCSC) Cloud Security Principles, and National Institute of Standards and Technology (NIST) Cloud Computing Standards.

Letter From our Chief Information Security Officer (CISO)

At Benchling, trust is part of our DNA. We believe that building trust is every bit as important as building the next game-changing product feature. Moreover, we believe that our continued investments in security, privacy, compliance, quality, and innovation all contribute to making Benchling a trustworthy partner.

The threats and risks faced by life science organizations are compounding every year. Security risks from apex-threat actors have become widespread. Regulatory risks are ballooning as governments around the world adopt stricter laws governing life sciences and technology. Life science organizations are finding it increasingly difficult to manage these risks with legacy software and systems — yet it's also difficult to adopt new technologies without knowing how trustworthy they are. Simply procuring functionality isn't enough; life sciences organizations must seek out software and systems that are secure, compliant, and that offer verifiable, consistent quality. Benchling has remained a leader in this space because we understand the importance of trust.

Benchling's investments and capabilities in security reach far beyond those of most software companies in the life sciences. We embed security engineers and security tools into every stage of our software development, from threat modeling with product designers to testing code for vulnerabilities prior to release. What's more, our teams work together to meet transparent security goals and requirements, as well as to uphold security engineering principles. We subject our systems to multiple penetration tests every year. Industry-leading security firms review our source code annually. From the CEO on down, every team at Benchling monitors, discusses, and prioritizes work based on security performance metrics — and we measure our work to the most stringent service-level objectives and control frameworks.

But producing secure code and products with enterprise-grade security features is just the beginning. We believe that investing in protection, detection, and responsiveness throughout our company is an investment in trust — which is why security is a crucial part of our culture at Benchling.

We hope to continue bringing Benchling's powerful, innovative products to an ever-growing circle of life science organizations — enabling groundbreaking research, development, and manufacturing advances, built on an unshakeable foundation of trust and security.

Zach Powers
Chief Information Security Officer

Introduction

The life science industry has witnessed tremendous innovation over the past decade. Gene and cell therapies, mRNA vaccines, plant-based meat, and innovative materials have all demonstrated significant progress toward harnessing biology for the advancement of humanity's wellbeing. As transformative as these innovations have been, the scientific techniques and R&D processes needed to bring them to market have sharply increased operational complexity, while exponentially multiplying the data generated by each project. Therefore, it has become more crucial than ever for life science organizations to manage and protect their data and information as a strategic asset.

Benchling addresses these needs by providing cloud-native software solutions designed to accelerate life sciences research and development. Hundreds of companies around the world rely on Benchling products to securely store, process, and analyze information pertaining to advancing life science products. These customers benefit from Benchling's ability to model complex scientific work, to adapt to their unique processes, and to centralize their data in ways that help drive new insights. Benchling's customers benefit from the cloud-native solution's inherent scalability, configurability, and interoperability with existing IT solutions.

Cloud software adoption has been steadily increasing within the life science industry throughout the past decade. This transformation has disrupted the traditional security relationship between vendors and customers, as vendors take on a much greater security responsibility than ever before. Benchling recognizes the burden of this responsibility, and maintains the highest standards of security and data protection to assure the security of customers' data. Furthermore, Benchling's customer-centric security-first approach is designed to make each product's capabilities easy to understand and integrate into existing operations throughout the customer organization. Customers leverage Benchling's products and services to enhance their ability to meet core security and privacy requirements, and to elevate their overall security posture.

This white paper reviews the security considerations most frequently considered when selecting software for corporate IT infrastructure. Benchling operates under a shared security responsibility model, and offers a comprehensive range of product controls, threat detection measures, disaster recovery procedures, data protection capabilities, and organizational policies to safeguard data for customers globally.

Product Security

Infrastructure Security and Engineering

Benchling utilizes Amazon Web Services (AWS) for hosting. AWS is a leader in infrastructure security, and maintains multiple security and compliance certifications including ISO 27001, SOC 1, and SOC 2 (as detailed here). Benchling's use of AWS enables the company to quickly iterate and test the quality, performance, and security of its systems — and to maintain control over the security of data, systems, and services within its computing environments. Benchling achieves this through measures such as configuration automation, vulnerability management, data and system backups, and preemptive threat detection.

A variety of network security controls, including network segmentation, firewalls, and traffic monitoring, are enforced within the production compute environments hosted on Benchling's AWS instances. In order to safeguard data from external threats, these production compute environments are isolated from the public internet, and are also segmented from the company's corporate enterprise networks. Benchling's approach to infrastructure engineering is centered around an infrastructure-as-code philosophy. This means security checks are embedded throughout all phases of the infrastructure engineering lifecycle. Furthermore, all code written by the company's infrastructure engineers is required to be reviewed, approved, and tested prior to release, to ensure it adheres to the highest quality, performance, and security standards.

Benchling's infrastructure is annually subjected to a wide range of different penetration tests, disaster recovery capability tests, and external audits. The company incorporates security- and privacy-by-design principles, embedding privacy and data protection concepts and the infrastructure engineering team throughout the lifecycle of all projects, from the initial design stages onward. Benchling's infrastructure is hardened based on security goals, National Institutes of Standards and Technology (NIST) standards, and Center for Internet Security (CIS) controls.

Software Development Life Cycle

Benchling's software engineering organization follows a standardized software development life cycle (SDLC), embedding security from the design phase all the way through the rollout of commercial products and features. All software engineers are trained on secure coding and application security tooling practices, ensuring that software development is both efficient and secure.

The company practices security- and privacy-by-design principles by incorporating threat and privacy modeling. Software and security teams provide multiple rounds of rigorous review during the design phase of all major features. Any changes to the code base require additional testing, review, and approval by a board of engineering experts prior to production.

Security tooling is integrated into Benchling's code pipeline, which incorporates a number of checks for application security vulnerabilities, such as static code analysis, dependency checking, and dynamic analysis. In addition, members of the security team regularly perform manual application security testing on key components. Any vulnerabilities discovered via these tests are routed through the software engineering work tracking system, and are governed by internal SLAs to ensure quick remediation and significantly reduce the risk exposure window.

Identity and Access Management

Within Benchling's solution, configurable controls enable customer administrators to customize each tenant's product security posture. Individual users can be configured using a granular permission structure, which offers flexible customer-admin defined user roles, along with the ability to grant specific types of access to external users. User access controls can be integrated with a customer's existing single sign-on (SSO) and multi factor authentication (MFA) systems, ensuring that only authorized individuals can access and make changes to the system — further enhancing security and mitigating risk. Additional security controls, such as IP range restrictions, can be enabled to restrict access to specific authorized IP addresses. For organizations that desire an additional layer of security, Benchling also provides rich application programming interfaces (APIs) that can be integrated with the customer's existing enterprise security systems.

All key actions performed within Benchling, such as logins, data writes and configuration changes, are attributable to particular users, and are captured with user information, date and time stamps in the audit logs.

Data Protection and Backup

Benchling's data records are designed not only for accuracy, but also for easy retrieval by customers, in accordance with the Electronic Record and Electronic Signature (ERES) requirements outlined in the 21 CFR Part 11 guidance. Benchling respects the privacy of customer data, and does not process or retrieve such data unless specifically instructed to do so by customer admins. All data and communication within Benchling is protected at rest using AES 256-bit encryption, and in transit using Transport Layer Security (TLS) encryption 1.2 or higher. By default, customer data is stored and processed in the United States, within a secure cloud environment hosted on AWS. Upon request, data storage and processing may be moved to other locations, such as within the E.U.

Within Benchling's AWS cloud environments, customer data is stored in S3 buckets, which provide granular, auditable control over data protection, along with programmatic verification of data security. Furthermore, Benchling's high-redundancy data storage practices ensure that the risk of customer data loss is minimized. Raw files are stored in S3 buckets which are designed for 99.999999999% durability over a given year. Structured data is stored in Postgres databases, which are configured with synchronous replication to encrypted daily and weekly backups. All content stored on Benchling's system is retained throughout the entire customer lifetime. Daily backups are kept for 35 days or more, to allow for granular data restoration, while weekly backups are kept for at least a year. Furthermore, encrypted backups are replicated across multiple geographic regions, providing greater redundancy.

Operational Security

Threat Detection

Benchling's data-driven approach to security focuses on the detection of anomalies in patterns of logged data. These high-fidelity alerts streamline threat detection, enabling more effective interventions. Furthermore, Benchling augments vendor-supplied alerts with its own proprietary threat models, which leverage key learnings uncovered during penetration-testing and red-team exercises.

Incident Response

While preventative measures remain an essential part of Benchling's overall strategy for diminishing overall incidents, not every attack can be prevented. For this reason, Benchling maintains a dedicated security incident response team, which works to minimize the impact of security events in near real-time, and leverages information obtained during each investigation to further strengthen Benchling's security posture. During an attack, the incident response team proceeds through the phases of Benchling's security incident response process and plan (IRP), which was created in alignment with the MITRE ATT&CK Framework and NIST.

The company ensures its readiness for an effective incident response by practicing and educating all internal teams on the correct tools and processes. Periodic tabletop exercises, utilizing realworld attack scenarios, are conducted with engineers and business leaders, enabling them to rehearse and fine-tune their responses. Key teams and individuals across the organization have been trained and armed with the right tools to contain, eradicate, and recover from an incident. Furthermore, the entire senior leadership team has a set of defined roles and responsibilities in the IRP, and receive annual training on security incident response.

Benchling takes its preparedness a step beyond even these measures, by conducting red-team exercises in which internal teams respond to manufactured threats they believe are genuine. The high degree of realism in these exercises enables the company to continuously test and refine each team's detection and response capabilities.

Disaster Recovery and Business Continuity Planning

Benchling maintains a thorough disaster recovery plan, as well as a business continuity plan. Annual testing ensures the company is prepared for black-swan events, and can continue to meet all customer commitments — including availability and performance SLAs, recovery time objectives (RTO), and recovery point objectives (RPO).

Benchling designs its products and services to remain resilient and effective under threat, understanding that external challenges are frequently unpredictable. The company's enterprise IT services and business workflows have also been planned and architected with these customer commitments in mind so customers' data is always safe.

Organizational Security

Enterprise Security

Benchling maintains ISO 27001 and Privacy Shield certifications, and complies with the GDPR as well as CCPA. Benchling aligns its security program and capabilities with the C5, NCSC Cloud Security Principles, and NIST Cloud Computing Standards.

The company's IT services are automated and compartmentalized to limit the security risk of any single component of the system. Benchling regularly tests, reviews, and monitors each step of its workflows, building detection and defense-in-depth into each of its IT services.

Benchling practices a Zero Trust policy. This means multiple security attributes are assigned to each Benchling team member and user account, and multi-factor authentication is required in order to access any of the company's IT services. A final layer of security is provided by the NIST Security Risk Management Framework, in which each security risk is assessed according to a set of internal benchmarks, with significant decisions requiring confirmation from Benchling's senior executive team.

Corporate compliance and security teams maintain procedures to ensure that vendors are reviewed and assessed for their quality and security, and that each vendor and external service receives careful oversight. The corporate compliance team conducts assessments, periodic reviews, and audits on all vendors, suppliers and contractors whose services may impact product or process quality.

In addition, Benchling undergoes annual security, privacy, and compliance audits by accredited external organizations — covering not only its products and customer-facing services, but also its enterprise security and IT services.

Security Training

All Benchling employees undergo security training as part of the orientation process, and receive ongoing security training yearly throughout their Benchling tenure. This training is focused on security and privacy policies, procedures, and best practices. Depending on an employee's job role, they may be required to undergo additional annual training on specific aspects of security, such as secure coding (in the case of software engineers). All training contains interactive components, such as modules on phishing, malware, and social engineering — requiring team members to engage with the material and demonstrate their understanding of potential threats.

Security Team

Benchling maintains a dedicated internal security team of security engineers, compliance experts, data engineers, and privacy- and incident-response professionals. This team is tasked with maintaining the company's defense systems, developing security review processes, building security infrastructure, and implementing Benchling's security policies. The team — whose members are actively involved in the global security industry, and possess extensive experience in the tech, government, and healthcare industries — also provides project-specific consulting services to Benchling's product and engineering teams.

The security team's data engineers are actively involved in Benchling's data modeling, acquisition, aggregation, and analysis, working to uphold confidentiality, integrity, and availability in each step of the company's robust threat detection process.

Privacy Program

Benchling's privacy program is managed jointly by a dedicated security, privacy and legal team. These experts ensure that the company's products reflect best-practice privacy standards, and adhere to the latest privacy regulations in all applicable countries and states. Furthermore, Benchling maintains a Privacy Shield certification, and maintains compliance with both GDPR and CCPA.

Governance

Benchling's posture on security, privacy, and compliance governance incorporates a declarative approach to policies and procedures, a data-driven approach to performance management, and a layered approach to risk mitigation.

Intensive annual external audits and assessments are performed on company's security, privacy, and compliance strategy, roadmap, capabilities, policies, and performance reports by accredited agencies. Leaders and team members throughout the company maintain ongoing discussions of Benchling's strategy and roadmap with senior leadership — helping develop programs for continuous improvement.

Management performs weekly reviews of all security, privacy, and compliance performance metrics against pre-set benchmarks and goals. Each security risk is assessed according to an internal risk management framework, with significant policy changes requiring approval from Benchling's senior executive team.

Conclusion

Benchling recognizes the crucial importance of its customers' intellectual property. As a result, the company has safeguarded this data with best-in-class standards of data security and protection. Across the product, operational, and organization levels, the company has implemented leading-edge security and privacy controls, and continues to invest in security and transparency throughout its operations.

For all these reasons, hundreds of life science organizations trust Benchling with their most valuable asset — their data — and utilize the company's products and services to strengthen their security posture. Benchling's dedicated security team welcomes questions and concerns at security@benchling.com, and strives to offer transparency to customers and potential customers alike.

www.benchling.com