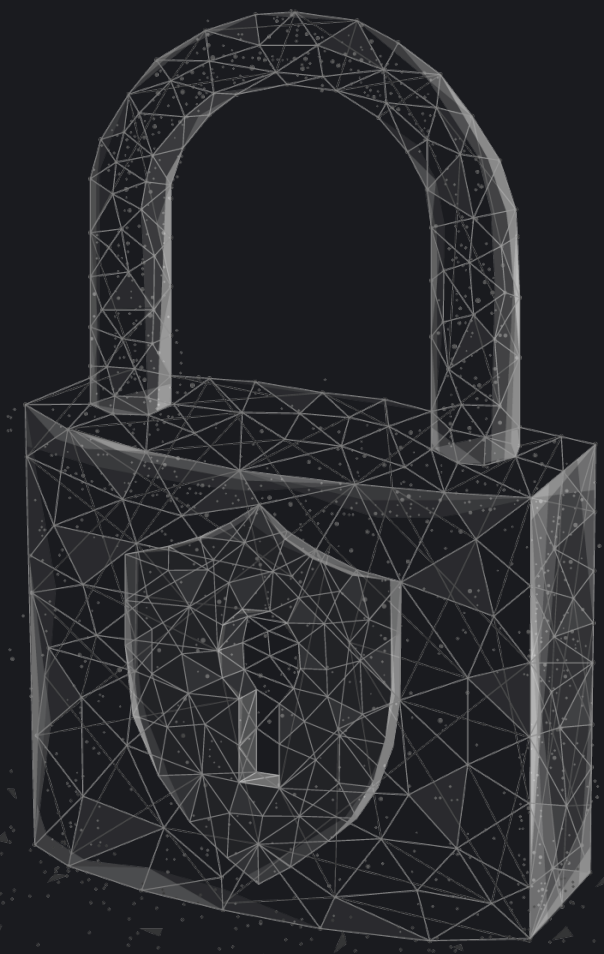

Markforged

Security at Markforged

Table of Contents

1 **Introduction** **02**

2 **Organizational Security** **02**

- Human Resource Security 02
- Physical Security 02
- Systems and Workstation Security 02
- Disaster Recovery and Incident Response 03
- Third-party Suppliers 03

3 **Protecting Customer Data** **03**

- Data Security and Encryption 03
- Data Segregation 03
- 2FA and Password Management 04
- Infrastructure 04
- Software 04

4 **Conclusion** **04**

5 **Terminology** **05**

Introduction

Our mission is to reinvent manufacturing with a 3D printing platform capable of producing strong parts for the factory floor. This mission is accomplished through combined efforts in advanced cloud computing, cutting-edge materials science, and best-in-class hardware engineering. Cloud computing is only possible when we prioritize the security of your data.

We are committed to being transparent about Markforged's security practices. We are continuously improving our security program, to ensure we are exceeding industry standards.

Organizational Security

Security is a company-wide priority at Markforged. We successfully completed our ISO 27001:2013 certification in 2019. This international standard for information security management systems serves as a baseline for our security controls and policies. Partnering with cybersecurity audit firm A-LIGN, we passed our ISO 27001 certification with zero major or minor nonconformities.

Risks, policies, and security plans are regularly reviewed by the Markforged Security team which is led by our CISO. Markforged leadership team is a crucial part of the security program. Our cross-functional security steering committee meets quarterly to drive security culture and address risk across the organization.

▸ Human Resource Security

We believe strong security starts with our employees. Comprehensive security training is delivered as part of an employee's first day at Markforged. Annual security awareness training is required for all employees thereafter.

All new employees are subject to background checks and must agree to confidentiality terms before joining the organization. Our IT and Human Resource teams work in tandem to ensure access to information and systems is limited to only what employees need to do their jobs.

▸ Physical Security

Access to our facilities is controlled by badge readers and is monitored by video surveillance. Secure and restricted areas that require additional training or contain sensitive information require approval to gain access permissions. Physical access audits are conducted quarterly.

▸ Systems and Workstation Security

As part of our standard IT onboarding, every Markforged employee is trained on the use of our corporate password management system to ensure unique and secure passwords are used organization-wide. To further reduce the risk of unauthorized access to our data and systems, multi-factor authentication is enforced on critical systems storing confidential or proprietary data.

All laptops and workstations issued to our employees are configured by the Markforged IT team and comply with the Markforged compute environment policy standards. This default configuration includes data encryption, passwords, antivirus enabled, and lock when idle. We require that all laptops and workstations be enrolled in management software supporting remote lock and wipe, as well security policy enforcement.

Disaster Recovery and Incident Response

Our disaster recovery and business continuity plans are reviewed and tested annually. Critical vendors and suppliers are evaluated with resilience and business continuity in mind. We have an incident response team responsible for responding to security incidents following our established policies and procedures. Our team runs incident response tabletop exercises annually to ensure readiness.

In the event of an incident affecting your data, we are committed to informing you via email or by posting on our status page.

Third-party Suppliers

Markforged leverages vendors and suppliers to provide the best experience for its customers. As part of the procurement process, Markforged evaluates the security posture of new vendors before use. When appropriate, Markforged establishes agreements with vendors that enforce the confidentiality commitments Markforged has made with its customers.

Quantitative risk assessments are conducted when onboarding new critical vendors. We evaluate their security posture ensuring controls commensurate with the sensitivity of the data they are accessing or storing are in place.

Protecting Customer Data

We understand the importance of protecting the part files and personal data you share with us. Protecting your data is top of mind as we work collaboratively to mitigate risk, iterate, and improve program standards.

Data Security and Encryption

We leverage FIPS 140-2 compliant encryption standards. All data is in transit using TLS. HTTPS is required for all services, including our public website and cloud applications. Additionally, your part files are protected with data encryption at rest by encrypting our Amazon Web Services (AWS) Simple Storage Service (S3) buckets where your part files are stored using AES-256. We have implemented controls to appropriately limit the creation, storage, usage, and deletion of encryption keys.

All print files sent to Markforged printers are formatted as Markforged Print files (MFP). MFP is an encrypted file format containing details about the part geometry, orientation, and fiber and material layout. This means that MFP files transferred from Eiger to Markforged printers by USB mass storage devices are secured via MFP encryption.

Data Segregation

Customer data is stored in our shared infrastructure, which is logically separated by unique customer IDs. Each time a database is queried to fetch customer data in an application, an API call containing that customer's unique ID is used to ensure segregation and security.

Using multi-tenant architecture allows us to ensure higher availability and system resilience while maximizing performance.

▸ 2FA and Password Management

Eiger provides users with the option to enable two-factor authentication (2FA) for additional security. Our 2FA utilizes time-based one time passwords (TOTP) and can be configured using well known 2FA apps like Google Authenticator or Authy.

User passwords are securely hashed, salted, and stored using AWS Cognito, which employs the SRP protocol.

▸ Infrastructure

All Markforged applications and data are hosted on Amazon Web Services (AWS). Markforged leverages AWS's infrastructure-as-a-service offerings to deliver highly available and resilient applications. AWS manages the security of all data center facilities, physical security of hardware, network infrastructure, and virtualization infrastructure. AWS maintains compliance with ISO 27001, SOC 2, and PCI frameworks. More information on AWS compliance and security can be found at https://aws.amazon.com/compliance/programs/.

Eiger, Markforged's cloud-connected print management software, manages cloud slicing of your parts using AWS's Lambda service. AWS Lambda enables Eiger to quickly scale and meet compute requirements while leveraging AWS's secure data centers. Customer part files are stored in AWS's S3 which provides unparalleled durability and data protection.

The AWS shared responsibility model for both Lambda and S3 leverage "serverless" architecture, meaning our software engineers do not have access to the underlying infrastructure. AWS is responsible for network and power redundancy, physical security, and operating system updates of the underlying infrastructure. This allows us to focus on creating enterprise-grade 3D printing software while AWS's security professionals mitigate infrastructure threats.

▸ Software

The Markforged software development lifecycle (SDLC) employs manual code reviews and automated integration testing before each deployment. Several pre-release environments are used for quality assurance and testing prior to releasing any Eiger code to production.

Markforged utilizes a continuous deployment model, which allows our customers to immediately benefit from new functionality, vulnerability remediation, and bug fixes.

In addition to internal testing and review, we contract with professional third-party penetration testers to evaluate our infrastructure configuration, IoT architecture, and Eiger code base annually. Summaries of these results are available upon request.

Conclusion

Data security is paramount at Markforged. Every engineer and designer who innovates with a Markforged printer expects their data and part files to be secure and confidential. Protecting that innovation is an obligation we take seriously and work diligently to uphold.

Terminology

AWS Lambda	Amazon Web Services Lambda is an event-driven, serverless computing platform. It is a computing service that runs code in response to events and automatically manages the computing resources required by that code.
TLS	Transport Layer Security (TLS) is a strong encryption protocol designed to protect communications on the Internet.
HTTPS	HyperText Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to.
AWS S3 Buckets	An Amazon Simple Storage Service (S3) bucket is a public cloud storage resource available in AWS. Amazon S3 buckets, which are similar to file folders, store objects, which consist of data and its descriptive metadata.
AES-256	Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). AES-256 is AES with a 256 bit key length.
Multi-tenant infrastructure	A single software environment which serves multiple tenants.
Two-factor authentication	Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.
PBKDF2	PBKDF2 is a "password-strengthening algorithm" that makes it difficult for a computer to check that any one password is the correct master password during a brute-force attack.
MFP	Markforged Print file (MFP) is an encrypted file type which is used to send details about the part geometry, orientation, and fiber and material layout from Eiger to Markforged printers.
Cloud Eiger	Eiger is Markforged's cloud-based 3D print software. It enables fiber routing and slicing once 3D CAD files are uploaded, access to print time and material cost estimates, global printer fleet management, and part file collaboration. Eiger is accessible at https://eiger.io/.