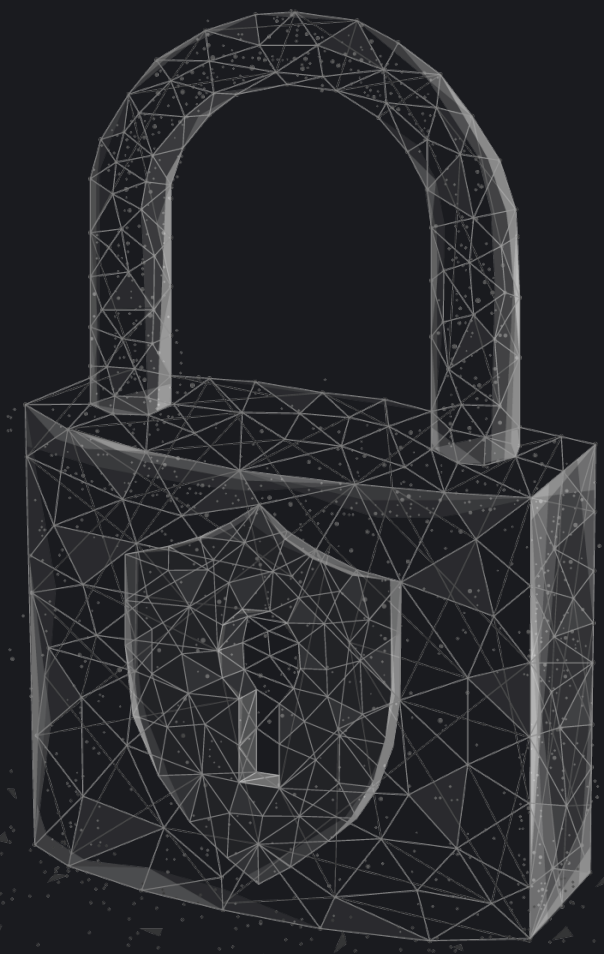

Markforged

Markforged의 보안

목차

소개

당사의 임무는 공장 현장에서 강력한 파트를 생산할 수 있는 3D 프린팅 플랫폼으로 제조를 재창조하는 것입니다. 이러한 임무를 달성하려면 고급 클라우드 컴퓨팅, 최첨단 재료 과학 및 동급 최강의 하드웨어 엔지니어링을 통합하는 노력이 필요합니다. 클라우드 컴퓨팅은 데이터 보안을 우선시할 때만 가능합니다.

당사는 Markforged의 보안 관행을 투명하게 유지할 것을 약속합니다. 보안 프로그램을 끊임없이 개선하여 언제나 당사의 표준이 업계 표준을 넘어설 수 있도록 노력하고 있습니다.

조직 보안

보안은 Markforged 전사를 통틀어 우선순위를 차지하는 목표입니다. 당사는 2019년에 ISO 27001:2013 인증을 획득하는 데 성공했습니다. 정보 보안 관리 시스템에 관한 이 국제 표준은 보안 통제 및 정책의 기준선 역할을 합니다. 사이버 보안 감사 회사인 A-LIGN과 협력하는 당사는 주요 또는 경미한 부적합 없이 ISO 27001 인증을 통과했습니다.

CISO가 이끄는 Markforged 보안 팀에서는 위험, 정책, 보안 계획을 정기적으로 검토합니다. Markforged의 리더십 팀은 보안 프로그램에서 중요한 부분을 차지합니다. 복합 기능 보안 조정 위원회는 분기별로 만나 보안 문화를 주도하고 범조직적인 위험을 해결합니다.

▸ 인적 자원 보안

강력한 보안은 직원으로부터 시작된다고 믿습니다. Markforged는 직원이 출근한 첫날 보안 교육을 포괄적으로 진행합니다. 이후 모든 직원이 빠짐없이 연간 보안 인식 교육을 받아야 합니다.

신입 직원은 모두 배경 조사를 받아야 하며 조직에 합류하기 전에 기밀 유지 조항에 동의해야 합니다. 당사의 IT 및 인사팀은 상호 협력하여 직원이 자기 업무를 수행하는 데 필요한 정보와 시스템에만 액세스할 수 있도록 제한합니다.

▸ 물리적 보안

당사는 배지 판독기를 사용해 시설에 대한 접근을 제어하며 감시 영상으로 모니터링합니다. 추가 교육이 필요하거나 민감한 정보가 포함된 보안 구역과 제한 구역에 액세스할 권한을 얻으려면 승인을 받아야 합니다. 분기별로는 물리적 액세스 감사를 실시합니다.

▸ 시스템 및 워크스테이션 보안

표준 IT 온보딩의 하나로 모든 Markforged 직원에게 기업 암호 관리 시스템 사용을 교육하여 조직 전체에서 안전한 암호를 사용할 수 있게 합니다. 당사 데이터 및 시스템에 대한 무단 액세스 위험을 더욱 줄이기 위해 기밀 또는 독점 데이터를 저장하는 중요한 시스템에 다중 인증을 적용합니다.

직원에게 지급되는 모든 노트북과 워크스테이션은 Markforged IT 팀에서 구성하고 Markforged 컴퓨팅 환경 정책 표준을 준수합니다. 이 기본 구성은 데이터 암호화, 암호, 바이러스 백신 활성화 및 유휴 시 잠금 등으로 이뤄집니다. 당사는 노트북과 워크스테이션을 모두 원격 잠금 및 삭제와 보안 정책 시행을 지원하는 관리 소프트웨어에 등록할 것을 요구합니다.

▸ 재해 복구 및 사고 대응

재해 복구 및 비즈니스 연속성 계획을 매년 검토하고 테스트합니다. 중요한 공급자와 공급업체를 탄력성과 비즈니스 연속성을 염두에 두고 평가합니다. 당사는 확립된 정책 및 절차에 따라 보안 사고에 대응할 책임이 있는 사고 대응팀을 두고 있습니다. 팀은 대응에 만전을 기하기 위해 매년 사고 대응 모의 훈련을 실시합니다.

사용자의 데이터에 영향을 미치는 사건이 발생하는 경우 이메일을 전송하거나 상태 페이지에 게시하여 사용자에게 알리기 위해 최선을 다하고 있습니다.

▸ 서드파티 공급업체

Markforged는 공급자와 공급업체를 활용하여 고객에게 최고의 경험을 제공합니다. Markforged는 조달 프로세스의 하나로 새로운 공급업체를 활용하기 전에 해당 업체의 보안 태세를 평가합니다. 적절한 경우 Markforged는 Markforged가 고객과 체결한 기밀 유지 협약을 시행하는 공급업체와 계약을 체결합니다.

새로운 중요 공급업체를 온보딩할 때는 정량적 위험 평가를 수행합니다. 우리는 업체의 보안 태세를 평가하여 그들이 액세스하거나 저장하는 데이터의 민감도에 상응하여 적소에서 상황을 제어하고 있는지 확인합니다.

고객 데이터 보호

당사는 고객이 당사와 공유하는 파트 파일과 개인 데이터 보호의 중요성을 알고 있습니다. 위험을 완화하고, 설계를 반복하고, 프로그램 표준을 개선하기 위해 협력할 때는 데이터를 보호하는 일이 가장 중요합니다.

▸ 데이터 보안 및 암호화

당사는 FIPS 140-2 호환 암호화 표준을 활용합니다. 모든 데이터는 TLS를 사용하여 전송하고 있습니다. 퍼블릭 웹 사이트와 클라우드 애플리케이션을 포함한 모든 서비스에 HTTPS가 필요합니다. 또한, 파트 파일을 AES-256로 저장하는 Amazon Web Services(AWS) Simple Storage Service(S3) 버킷을 암호화하는 방식으로 데이터를 암호화하여 사용하지 않는 파트 파일을 보호합니다. 당사는 암호화 키의 생성, 저장, 사용, 삭제를 적절하게 제한하는 제어 기능을 구현했습니다.

Markforged 프린터로 전송되는 프린팅 파일은 모두 Markforged Print 파일(MFP) 형식입니다. MFP는 암호화된 파일 형식이며 파트 형상, 방향, 섬유, 재료 레이아웃에 대한 세부 정보가 포함되어 있습니다. 이는 USB 대용량 저장 장치를 통해 Eiger에서 Markforged 프린터로 전송된 MFP 파일을 MFP 암호화로 보호한다는 의미입니다.

▸ 데이터 분리

고객 데이터를 고유한 고객 ID로 논리적으로 분리된 공유 인프라에 저장합니다. 애플리케이션에서 고객 데이터를 가져오기 위해 데이터베이스를 쿼리할 때마다 해당 고객의 고유 ID가 포함된 API를 호출하여 데이터를 분리하고 보안을 유지합니다.

다중 테넌트 아키텍처를 사용하면 최고의 성능을 유지하면서 더 우수한 가용성과 시스템 복원력을 보장할 수 있습니다.

▸ 2FA 및 비밀번호 관리

Eiger에서는 사용자가 추가 보안을 위해 2단계 인증(2FA)을 활성화할 수 있는 옵션을 사용할 수 있습니다. 당사의 2FA는 시간 기반 일회용 비밀번호(TOTP)를 사용하며 Google Authenticator 또는 Authy와 같이 잘 알려진 2FA 앱을 사용하여 구성할 수 있습니다.

사용자 암호는 SRP 프로토콜을 사용하는 AWS Cognito를 사용하여 안전하게 해시, 솔트, 저장합니다.

▸ 인프라

모든 Markforged 애플리케이션 및 데이터는 Amazon Web Services(AWS)에서 호스팅됩니다. Markforged는 AWS의 서비스형 인프라스트럭처(IaaS, infrastructure-as-a-service) 제품을 활용하여 가용성이 높고 복원력이 좋은 애플리케이션을 제공합니다. 당사는 AWS로 모든 데이터 센터 시설의 보안, 하드웨어의 물리적 보안, 네트워크 인프라, 가상화 인프라를 관리합니다. AWS는 ISO 27001, SOC 2, PCI 프레임워크를 준수합니다. AWS 규정 준수 및 보안에 관한 자세한 내용은 https://aws.amazon.com/compliance/programs/에서 확인할 수 있습니다.

Markforged의 클라우드 연결 프린팅 관리 소프트웨어인 Eiger는 AWS의 Lambda 서비스를 사용하여 파트의 클라우드 슬라이싱을 관리합니다. Eiger는 AWS Lambda를 통해 AWS의 보안 데이터 센터를 활용하는 한편 신속하게 확장하고 컴퓨팅 요구 사항을 충족할 수 있습니다. 고객의 파트 파일은 탁월한 내구성과 데이터 보호를 제공하는 AWS의 S3에 저장됩니다.

Lambda와 S3 모두에 대한 AWS 공유 책임 모델은 "서버리스" 아키텍처를 활용합니다. 즉, 당사의 소프트웨어 엔지니어가 기본 인프라에 액세스할 수 없습니다. AWS는 기본 인프라의 네트워크 및 전력 이중화, 물리적 보안, 운영 체제 업데이트를 담당합니다. 이로써 AWS의 보안 전문가는 인프라 위협을 완화하는 동안 엔터프라이즈급 3D 프린팅 소프트웨어를 만드는 데 집중할 수 있습니다.

▸ 소프트웨어

Markforged의 소프트웨어 개발 수명 주기(SDLC)에서는 각 배포 전에 수동 코드 검토 및 자동화된 통합 테스트를 사용합니다. Eiger 코드를 프로덕션에 릴리스하기 전에 다양한 시험판 환경에서 품질 보증 및 테스트를 진행합니다.

Markforged는 지속적인 배포 모델을 활용하므로 고객은 새로운 기능, 취약성 수정 및 버그 수정의 이점을 즉시 누릴 수 있습니다.

내부 테스트 및 검토 외에도 전문적인 서드파티 침투 테스터와 계약하여 인프라 구성, IoT 아키텍처 및 Eiger 코드 기반을 매년 평가합니다. 해당 평가 결과 요약 보고서를 요청 시 제공합니다.

결론

Markforged는 데이터 보안을 가장 중요하게 여깁니다. Markforged 프린터로 혁신을 이루려는 엔지니어와 설계자는 모두 데이터와 파트 파일을 안전하게 보관하고 기밀로 유지되기를 바랍니다. 이러한 혁신을 보호하는 책무를 당사는 진지하게 받아들이고 또 유지하기 위해 성실하게 노력하고 있습니다.

용어

AWS Lambda	Amazon Web Services Lambda는 이벤트 중심의 서버리스 컴퓨팅 플랫폼입니다. 이벤트에 대한 응답으로 코드를 실행하고 해당 코드에 필요한 컴퓨팅 리소스를 자동으로 관리하는 컴퓨팅 서비스입니다.
TLS	전송 계층 보안(TLS)은 인터넷에서 통신을 보호하도록 설계된 강력한 암호화 프로토콜입니다.
HTTPS	하이퍼 텍스트 전송 프로토콜 보안(HTTPS)은 브라우저와 접속한 웹사이트 간에 데이터가 전송되는 프로토콜인 HTTP의 보안 버전입니다.
AWS S3 버킷	Amazon Simple Storage Service(S3) 버킷은 AWS에서 사용할 수 있는 퍼블릭 클라우드 스토리지 리소스입니다. 파일 폴더와 유사한 Amazon S3 버킷에는 데이터와 설명 메타데이터로 구성된 객체를 저장합니다.
AES-256	고급 암호화 표준(AES)은 미국 국립표준기술연구소(NIST)에서 제정한 전자 데이터 암호화 사양입니다. AES-256은 키 길이가 256비트인 AES입니다.
다중 테넌트 인프라	다중 테넌트에 서비스를 제공하는 단일 소프트웨어 환경입니다.
2단계 인증	2단계 확인, 때로는 이중 인증이라고도 하는 2단계 인증(2FA)은 사용자가 자신을 확인하기 위해 두 가지 다른 인증 요소를 제공하여 사용자 자격 증명과 사용자가 접근할 수 있는 리소스를 모두 더 안전하게 보호하는 보안 프로세스입니다.
PBKDF2	PBKDF2는 무차별 대입 공격 시 컴퓨터가 올바른 마스터 암호가 어떤 것인지 확인하기 어렵게 만드는 "암호 강화 알고리즘"입니다.
MFP	Markforged Print 파일(MFP)은 Eiger에서 Markforged 프린터로 파트 형상, 방향, 섬유 및 재료 레이아웃에 대한 세부 정보를 보내는 데 사용되는 암호화된 파일 유형입니다.
Cloud Eiger	Eiger는 Markforged의 클라우드 기반 3D 프린팅 소프트웨어입니다. 3D CAD 파일을 업로드하면 파이버 라우팅 및 슬라이싱, 프린팅 시간 및 재료 비용 추정, 글로벌 프린터 제품군 관리 및 파트 파일 협업에 액세스할 수 있습니다. Eiger는 https://eiger.io/를 통해 접근할 수 있습니다.