monday.com
보안 및 개인정보 보호 백서

날짜	버전	변경 설명
2021년 11월	1.0	최종 버전

이 백서는 이 백서 발행일 현재 존재하는 monday.com의 보안 및 개인정보 보호 관행에 대한 개요를 제공하기 위한 것으로 사전 알림 없이 변경될 수 있습니다. 향후 계획에 대한 설명은 monday.com의 단독 재량에 따라 변경되거나 지연될 수 있습니다. 이 백서는 정보 제공의 목적으로만 사용되며 법적 조언을 구성하거나 계약상의 동의 조건을 보완하거나 포함하는 것으로 인식되지 않습니다.

목차

1. 소개

monday.com Work OS는 전 세계 127,000개 이상의 회사 데이터를 관리하며 이러한 책임을 가지고 고객에게 최고 수준의 보안 및 데이터 보호를 제공하기 위해 최선을 다하고 있습니다. 당사는 데이터 보안을 최우선으로 하여 고객의 신뢰를 얻고 있습니다.

사명 선언문

monday.com Work OS에서 데이터를 관리하는 동안 고객은 당사를 믿고 안심할 수 있습니다.

운영팀

monday.com의 정보 보안 노력은 인프라, R&D, 운영 및 IT 팀의 대표로 구성된 보안 포럼과 CISO 및 보안팀이 안내하고 모니터링합니다.
monday.com의 개인정보 보호 노력은 법률, 개인정보 및 보안팀의 대표로 구성되고 DPO가 이끄는 개인정보 포럼에 의해 안내 및 모니터링됩니다.

유용한 링크

monday.com 신뢰 센터
monday.com 법률 포털
monday.com의 상태 페이지
하위 프로세서, 자회사 및 지원
monday.com의 보안 및 개인정보 보호 - 자주 묻는 질문
취약점 보고
지원 및 기술 자료
가격 체계 및 플랜
monday.Engineering 블로그

---

2. 인프라 보안

호스팅 제공업체

당사의 서비스는 고가용성 및 복원력을 달성하기 위해 여러 가용 영역에 걸쳐 다른 지역에 구축된 전용 재해 복구(DR) 배포와 함께 주로 미국 북부 버지니아 및 독일 프랑크푸르트와[1] 같은 여러 지역의 아마존 앱 서비스 인프라(AWS)에서 호스팅됩니다. 고객 계정은 단일 지역에 소속됩니다.

AWS 공동 책임 모델에서 AWS는 클라우드 컴퓨팅 인프라의 보안을 관리하고 monday.com은 클라우드 컴퓨팅 인프라에 있는 소프트웨어 및 데이터의 보안을 관리합니다.

활동 로그 기능(이 문서에서 자세히 설명)은 GCP(미국 구글 클라우드 플랫폼)에 데이터를 백업합니다.

네트워크 구조

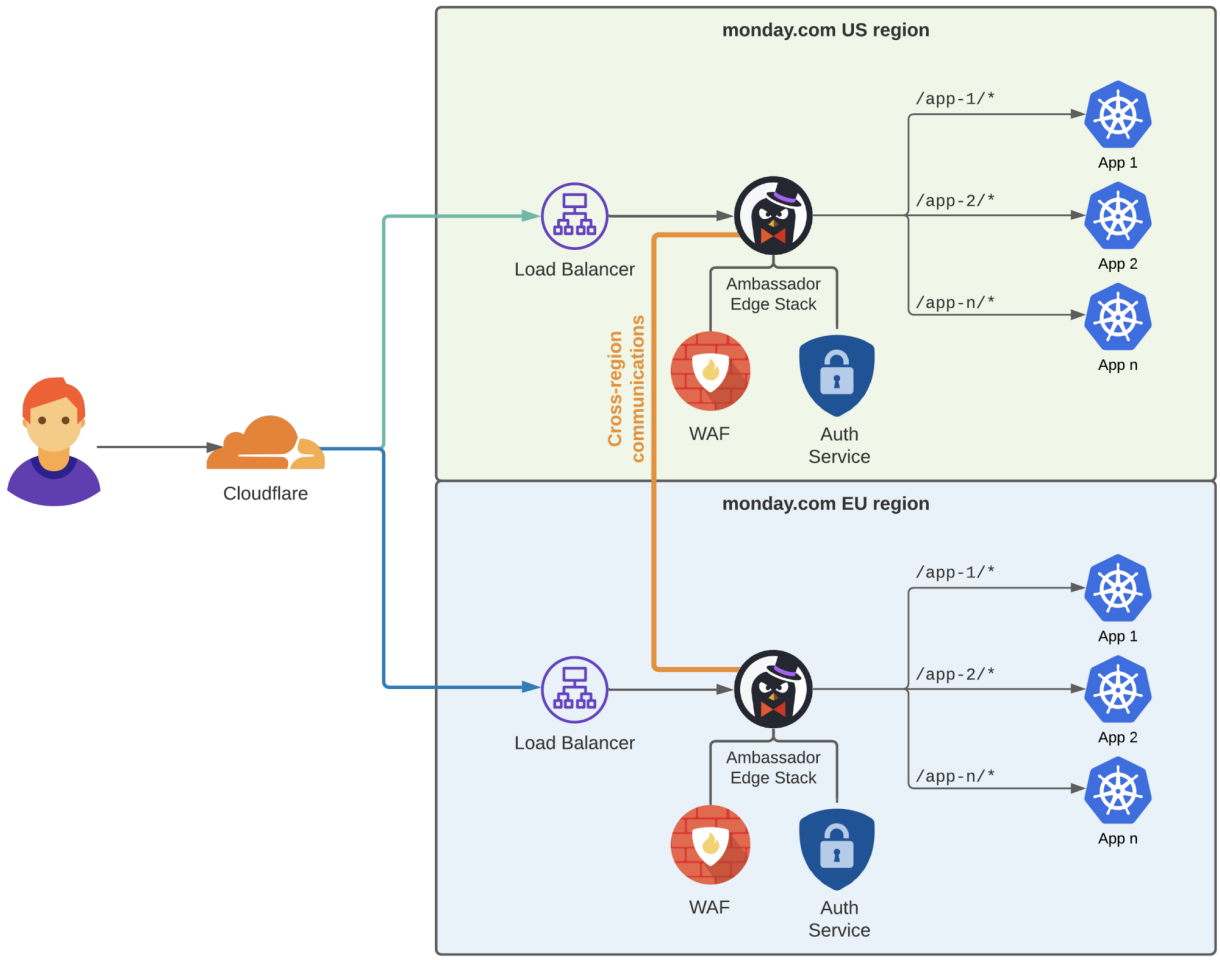
- monday.com의 네트워크 구조는 퍼블릭 서브넷과 프라이빗 서브넷을 분리하는 것을 포함하여 AWS 모범 사례에 따라 구축되었습니다.
- monday.com은 Cloudflare 및 Fastly를 비롯한 여러 CDN 제공업체를 사용하여 DDoS 공격 및 무차별 대입 공격을 방지합니다. 속도 제한은 엣지와 애플리케이션 수준 모두에서 구성됩니다.
- 로드 밸런서는 퍼블릭 서브넷에 있는 반면 웹 애플리케이션 서버 및 데이터베이스와 같은 내부 네트워크 구성 요소는 프라이빗 서브넷에 있으며 할당된 퍼블릭 IP가 없습니다.
- 콘텐츠 기반 동적 공격 차단을 위해 웹 응용 프로그램 방화벽(WAF)이 설치되어 있습니다.
- 방화벽은 네트워크 리소스에 대해서만 허용된 포트를 통해 액세스하고 IP 화이트리스트를 적용하기 위해 네트워크 전체에서 사용됩니다. 보안 그룹 규칙은 필수 포트에서만 액세스를 허용하도록 구성됩니다.
- 네트워크 침입 탐지 시스템(NIDS) 센서는 모든 프로덕션 자산에 대해 활성화된 기본 AWS 보안 서비스와 함께 사용됩니다.

다음은 미국 데이터 영역과 EU 데이터 영역 모두에서 monday.com의 네트워크 다이어그램의 하이라이트 부분을 나타냅니다:[2]

---

[1] 엔터프라이즈 플랜 고객은 독일 프랑크푸르트에 있는EU 데이터 센터의 데이터 호스팅을 선택할 수 있습니다.

[2] 높은 수준의 그리드 네트워크 다이어그램은 수요 및 MNDA 서명에 따라 공유될 수 있습니다.



코드형 인프라는 구성 변경 사항을 추적하고 감사할 수 있도록 광범위하게 사용됩니다. monday.com의 인프라 팀은 분기별로 경계 네트워크 구성을 철저히 검토하고 보안을 유지하거나 강화하는 데 필요하다고 판단되는 사항을 변경합니다.

AWS 첨단 기술 파트너

monday.com은 AWS 첨단 기술 파트너이며, 이는 AWS가 당사 조직을 인프라, 정보 보안, 모범 사례 설계 등의 측면에서 엄격하게 심사했음을 증명하는 것입니다.

네트워크 보안

monday.com은 순전히 클라우드 기반 솔루션이므로 최신 클라우드 지향 컨트롤을 사용하여 네트워크 경계를 정확하게 파악할 수 있는 이점이 있습니다. NIDS를 사용하여 네트워크 로그와 엣지 로케이션의 트래픽 로그를 수집 및 모니터링하고 보안 정보 및 이벤트 관리(SIEM) 시스템을 통해 관련 경보를 검토합니다. 당사는 클라우드 공급자로부터 보안 그룹 및 네트워크 ACL 구성을 자주 검색하고 네트워크의 전체 개요를 구성하는 보안 모니터링 도구를 사용합니다.

monday.com의 인프라 팀은 분기별로 경계 네트워크 구성을 철저히 검토하고 보안을 유지하거나 강화하는 데 필요하다고 판단되는 사항을 변경합니다. 또한, 당사는 네트워크 구성을 검토하기 위해 매년 독립적인 감사 업체와 협력합니다.

프로덕션 액세스

프로덕션 자산에 대한 액세스 권한은 역할에 따라 그리고 알 필요 및 최소 권한 원칙에 따라 부여됩니다. 관리 권한은 인프라 팀 직원(제한된 소규모의 숙련된 엔지니어 팀)에게만 제공됩니다. monday.com 서버에 대한 모든 액세스는 VPN을 사용해야 하며, 이 VPN은 엔터프라이즈 ID 공급자(IdP)에 대해 인증되고 완전히 감사되며 비밀번호 강도 및 다단계 인증(MFA)을 시행합니다. 개발자의 프로덕션 자산에 대한 액세스는 쿠버네티스 포트 전달을 사용하여 실행되며 IdP에 대해서도 이와 유사하게 인증됩니다.

강화

서버는 인터넷 보안 센터(CIS) 표준에 따라 강화된 최신 Ubuntu LTS 버전(20.04)을 기반으로 합니다.

데이터베이스

monday.com에서 사용하는 데이터베이스에는 MySQL, Elasticsearch 및 Redis가 있습니다. 통합 기능에서 사용하는 외부 시스템에 대한 API 키는 자체 복제 전용 HashiCorp Vault 클러스터에 저장됩니다.

파일 저장

파일 스토리지는 첨부 파일과 데이터베이스 백업을 저장하는 AWS의 간편 보관 서비스(S3)에서 호스팅됩니다. 첨부 파일에는 고객이 monday.com 서비스에 업로드한 모든 파일이 포함됩니다.
monday.com은 사용자가 서비스에 업로드한 파일에 대해 자동화된 악성코드 탐지 서비스를 제공하여 서비스에 업로드된 외부 파일이 감염되지 않도록 합니다. 또한 금지된 파일 확장자 목록이 포함된 블랙리스트가 있습니다. 파일 확장자 블랙리스트에는 실행 파일이나 HTML과 같이 위험한 것으로 간주될 수 있는 파일 형식이 포함되어 있습니다. 이러한 파일 형식을 차단하여 악성코드의 감염 위험을 크게 줄입니다.

다중 지역

2021년 1월부터 monday.com은 독일 프랑크푸르트의 첫 번째 유럽 데이터 지역으로 확장되었습니다(현재 엔터프라이즈 플랜 고객에게 제공됨).
미국 지역의 인프라 원칙으로 EU의 monday.com 고객도 동일한 수준의 보안 조치 및 통제와 기밀성, 무결성 및 가용성의 CIA 3원칙이 준수된다는 확신을 가지고 monday.com 경험을 누릴 수 있습니다.
monday.com 네트워크 다이어그램의 주요 내용은 위에 설명되어 있습니다.
앞으로 다른 지역에도 데이터 센터를 열 계획입니다.

암호화 및 키 관리

전송 중 암호화

개방형 네트워크를 통해 전송 중인 데이터는 TLS 1.3(최소 TLS 1.2)을 사용하여 암호화됩니다.

저장 데이터 암호화

미사용 데이터는 AES-256을 사용하여 암호화됩니다. 암호화 키는 AWS의 키 관리 서비스(KMS)를 사용하여 저장됩니다. 매년 순환되는 고객 마스터 키(CMK)는 현재 monday.com 서비스에 제출되어 고객을 대신해 처리하는 모든 고객 데이터를 암호화하는 데 사용됩니다.

테넌트 분리

당사의 환경은 고객이 논리적으로 분리된 다중 테넌트입니다. 고객 데이터는 여러 매개변수 조합의 결과인 고유 ID를 사용하여 애플리케이션 수준에서 분리됩니다.

당사는 현재 고객을 위해 테넌트 수준 암호화(TLE)를 활성화하기 위해 노력하고 있습니다. TLE는 미사용 데이터가 계정별 고유 전용 키로 암호화되도록 보장하고 권한이 없는 시스템이나 직원이 데이터를 보는 것을 방지하는 하나의 층입니다.

TLE는 두 가지 주요 시나리오로부터 보호합니다:

1. **공격자:** 데이터베이스 필드의 데이터는 암호화되므로 공격자가 데이터베이스에 액세스하고 데이터를 추출할 경우 암호화된 데이터만 제공됩니다.
2. **우발적 공유:** 데이터는 계정별 전용 키로 암호화되므로 실수로 계정 간에 데이터를 공유하는 경우 일반 텍스트로 공유되지 않습니다.

향후 엔터프라이즈 플랜 고객에게 자신의 암호화 키(BYOK: 자체 키 가져오기)를 가져올 수 있는 옵션을 제공할 계획입니다.

백업

monday.com은 고객이 monday.com 서비스에 제출한 데이터를 고객을 대신하여 처리하고 백업합니다. 5분마다 사용자 데이터를 일관되게 백업하고 여러 AWS 가용 영역에 암호화된 백업을 배포합니다. 또한 중복을 대비해 별도의 AWS 지역에 DR 사이트를 구축했습니다. 활동 로그 데이터는 GCP에 백업됩니다.

확장성 및 안정성

마이크로서비스 구조는 하나 이상의 구성 요소에 장애가 발생한 경우 시스템의 건전성에 미치는 영향을 최소화하기 위해 활용됩니다. monday.com 서비스는 오케스트레이션에 쿠버네티스를 사용하여 완전히 컨테이너화됩니다. 이는 최종 사용자에게 양질의 경험을 제공하는 동시에 증가하는 고객 요구를 처리하는 데 적합한 확장성이 뛰어난 인프라를 제공합니다.

코드형 인프라는 인프라 리소스의 가청성과 유지 관리 가능성을 보장하기 위해 테라폼을 통해 널리 사용됩니다.

monday.com은 모든 인프라 구성 요소에 대한 성능 메트릭을 지속적으로 모니터링하고 규모에 맞게 인프라를 구축합니다. 또한 당사의 로드맵이 점점 더 많은 고객에게 양질의 서비스와 프로덕션의 기능을 제공할 수 있도록 인프라 엔지니어 및 경영진과 함께 분기별 규모 검토를 실시합니다.

서비스 수준 계약(SLA)

서비스의 가용성은 상태 페이지를 통해 모니터링할 수 있습니다. 유지보수를 위한 시스템 가동 중지 시간은 거의 필요하지 않습니다. 유지보수가 필요한 경우 가능한 한 주말에 활동이 적은 시간에 일정이 잡습니다.

가동 중지 시간에 대한 알림은 상태 페이지를 통해 즉시 확인할 수 있습니다. 고객은 이메일 또는 문자 메시지를 통해 가용성 및 당사 팀의 완화 노력에 대한 알림을 구독할 수 있습니다.

엔터프라이즈 플랜 고객에게는 99.9% 가동 시간을 약속합니다.

---

3. 보안 기능 및 다른 기능

인증

monday.com은 다음 인증 방법을 지원합니다:

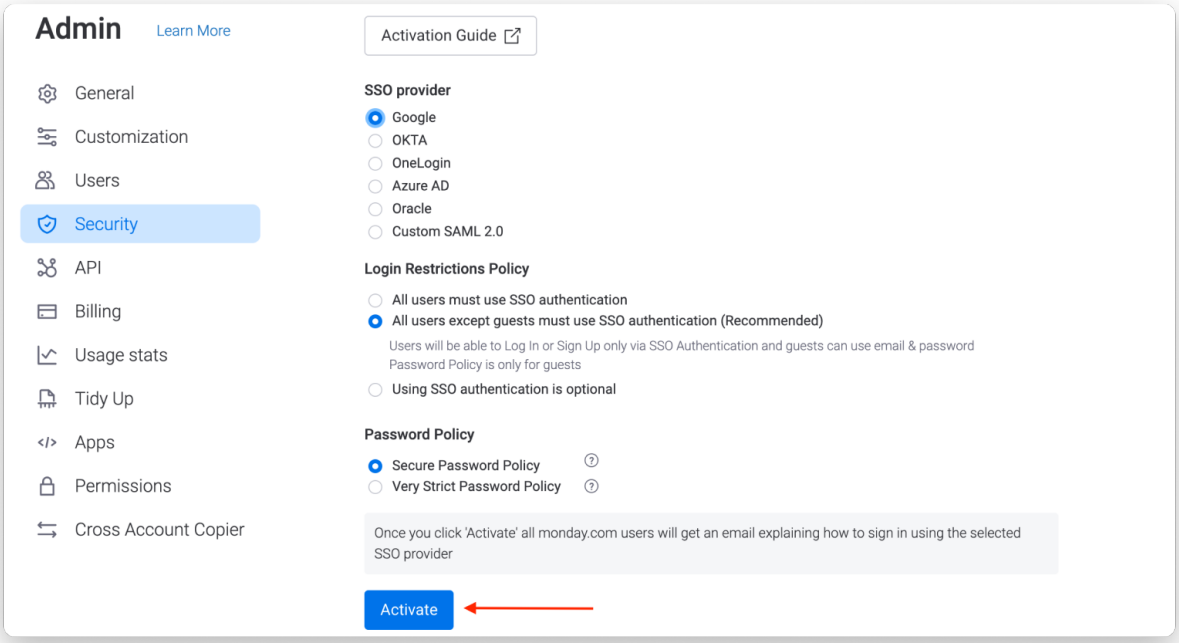
자격 증명

자격 증명을 사용하여 계정 사용자를 인증하도록 선택한 경우 관리자는 계정에 대해 두 가지 암호 강도 설정을 선택할 수 있습니다:

1. 반복 또는 연속 문자가 없는 최소 8자, 또는
2. 반복 또는 연속 문자가 없는 최소 8자로 최소 하나의 숫자(1, 2, 3), 하나의 소문자(a, b, c) 및 하나의 대문자(A, B, C)를 포함해야 합니다.

Google 통합 인증(SSO)

Google SSO는 사용자가 Google 계정을 사용하여 monday.com 서비스에 로그인할 수 있도록 하여 여러 비밀번호를 기억해야 하는 부담을 줄이는 보안 인증 시스템입니다.
이 기능은 프로 및 엔터프라이즈 플랜에서만 사용할 수 있습니다.



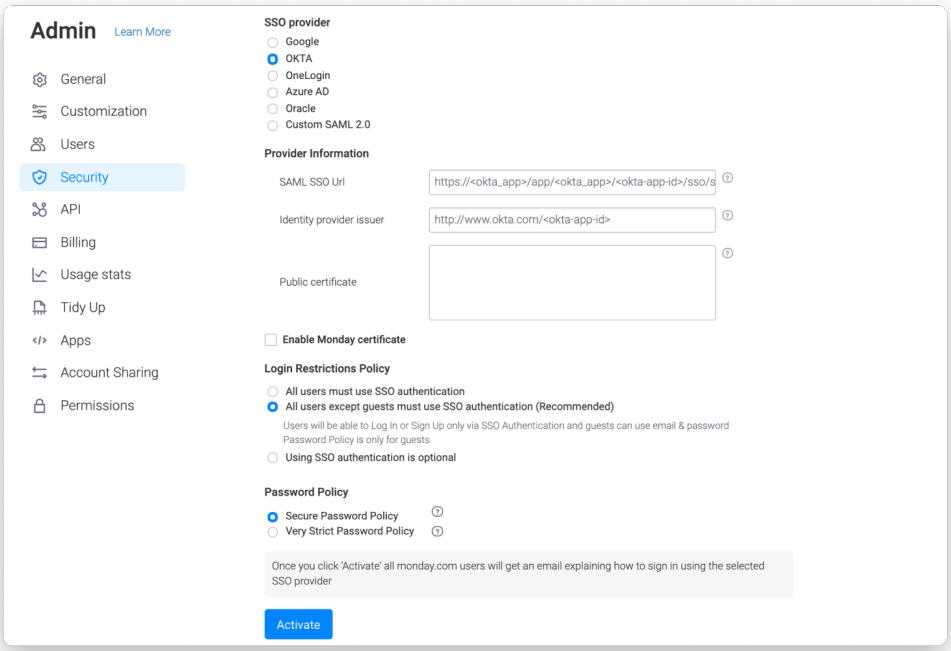
ID 제공자(IdP)

monday.com은 현재 세 가지 주요 ID 제공자를 지원합니다:

1. OKTA

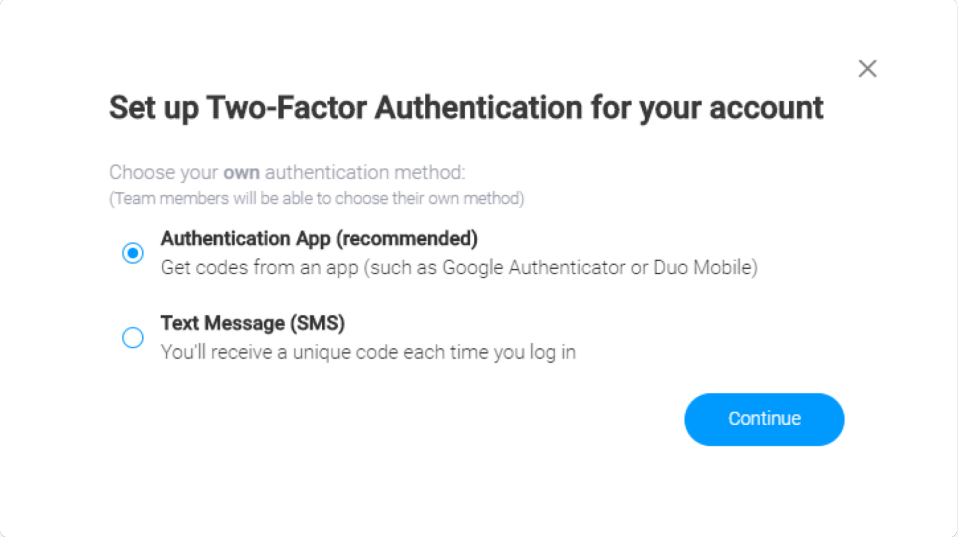
2. Azure AD
3. OneLogin

또한 고객은 사용자 지정 SAML 2.0을 사용하여 자체 공급자를 사용할 수 있습니다.
이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.



이중 인증 (2FA)

위의 인증 방법 외에도 관리자는 추가 보안 계층을 구성하고 문자 메시지(SMS) 또는 인증 앱을 통해 2FA를 활성화할 수 있습니다.
IdP와 통합하기로 선택한 경우 2FA가 사용자 측에서 활성화되어야 합니다.



인증

SCIM 프로비저닝

교차 도메인 ID 관리를 위한 시스템(SCIM)은 여러 애플리케이션에서 사용자 관리를 위한 프로토콜로, 이를 통해 여러 애플리케이션에서 사용자 및 팀 데이터를 한 번에 쉽게 프로비저닝(추가), 프로비저닝 해제(비활성화) 및 업데이트를 할 수 있습니다. monday.com은 SCIM 프로비저닝을 설정하는 세 가지 방법을 지원합니다:

1. 기존 monday.com SCIM 애플리케이션:
    a. OKTA
    b. Azure AD
    c. OneLogin
2. 선택한 ID 공급자와 맞춤형 SCIM 통합
3. API를 사용한 SCIM 프로비저닝

다음 표는 monday.com의 SCIM 통합에서 지원되는 모든 **사용자** 속성을 나타냅니다:

monday.com 속성	SCIM API 속성	설명
이름(필수)	이름, 표시이름	사용자의 표시 이름.
이메일 주소(필수)	사용자이름, 이메일	사용자가 monday.com 서비스에 로그인하는 데 사용하는 이메일 주소입니다.
활동(필수)	활동	사용자를 생성할 때 이 필드는 '참'로 설정되어야 합니다. 사용자의 '활동' 값을 '거짓'으로 변경하면 monday.com 서비스에서 비활성화됩니다.
직위	직위	조직 내 사용자의 직위

시간대	시간대	사용자의 시간대(플랫폼의 모든 날짜는 이 시간대를 따릅니다).
로케일	로케일	monday.com은 다른 로케일에 대해 현지화된 버전을 표시합니다.
전화 번호	전화번호	사용자의 전화번호('기본'으로 지정한 전화번호만 표시됨).
집 주소	주소	사용자의 주소('기본'으로 지정한 주소만 표시됨).
사용자 유형	사용자유형	계정 내 각 사용자의 수준입니다. 가능한 값은 관리자, 구성원, 시청자 또는 게스트입니다(기본값은 "구성원").

다음 표는 monday.com의 SCIM 통합에서 지원되는 모든 **팀** 속성을 나타냅니다:

monday.com 속성	SCIM API 속성	설명
이름(필수)	표시이름	팀의 표시 이름입니다.
사용자	구성원	팀에 할당된 사용자 목록입니다.

이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.

권한

monday.com은 귀하의 계정에서 누가 무엇을 할 수 있는지 제어하는 데 도움이 됩니다. 당사는 다음을 포함하여 데이터 보기 또는 편집을 제한하도록 사용자 정의할 수 있는 여러 유형의 권한을 제공합니다

1. **보드 권한**
    a. 유형: "메인", "공유 가능" 및 "비공개" 보드
    b. 제한 사항: "모든 항목 편집", "콘텐츠 편집", "담당자가 편집" 및 "보기 전용"
2. **칼럼 권한:** "칼럼 편집 제한" 및 "칼럼 보기 제한"
3. **대시보드 권한**
    a. 유형: "메인", 및 "비공개" 대시보드
    b. 제한 사항: 대시보드 소유자만 대시보드와 그 안에 있는 앱 및 위젯을 편집할 수 있습니다.
4. **작업 공간 권한**
    a. 유형: "개방형" 및 "폐쇄형" 작업 공간
    b. 제한 사항: "아무도 없음", "관리자만", "작업 공간 소유자" 및 "누구나"

5. **계정 권한:** 관리자는 다음 기능에 대한 제한("아무도 없음", "관리자만" 및 "모든 사람")을 설정할 수 있습니다:
    a. 파일 업로드
    b. 브로드캐스트 보드
    c. 메인 보드 생성
    d. 비공개 보드 생성
    e. 공유 보드 생성
    f. 통합 생성
    g. 자동화 생성
    h. 작업 공간 생성
    i. 계정의 모든 사용자를 업데이트 또는 보드에 언급하거나 기명
    j. 보드, 활동 로그 , 검색 결과 및 업데이트를 Excel로 내보내기

위의 기능 중 일부는 모든 플랜에서 사용하지 못할 수도 있습니다.

monday.com 내 역할

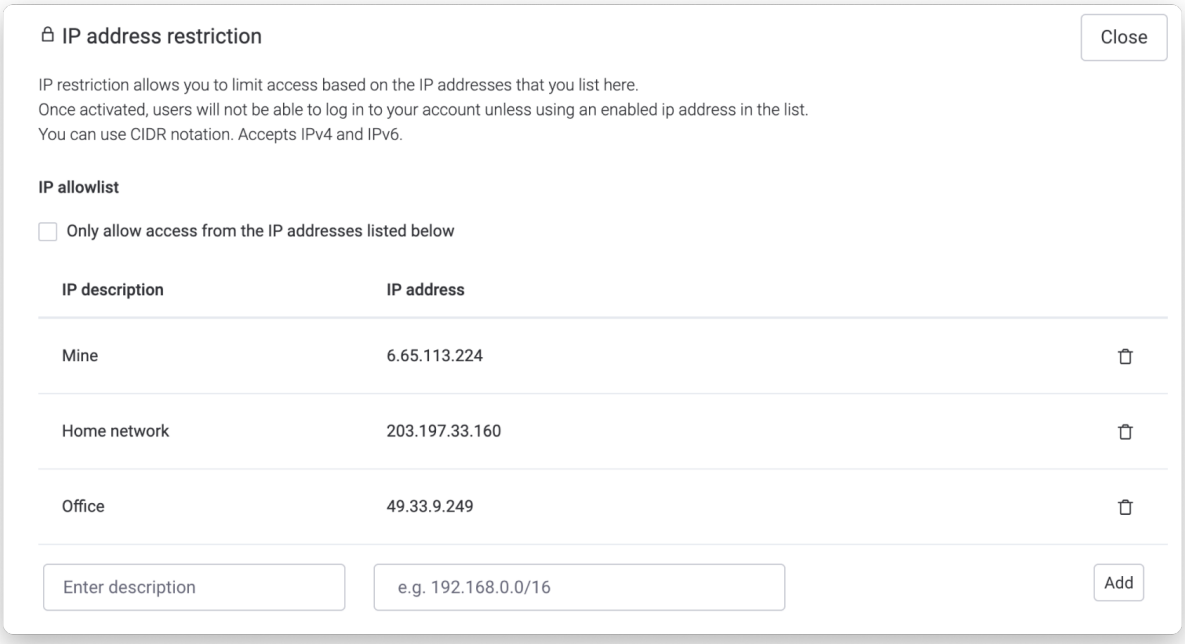
monday.com 내 역할은 다음과 같습니다:

역할	설명	가능	불가능
관리자	팀을 관리하는 팀 구성원(선택한 경우 그 이상)	전체 계정 감독 사용자 및 보드에서 보안 및 청구에 이르기까지 모든 것을 관리함(아래 "관리자 패널" 섹션에 설명됨)	
구성원	수정 권한이 있음 (초대할 수 있는 회원 수는 플랜에 따라 다름)	• 보드, 항목 및 폴더 생성 및 편집 • 보드 및 항목 내에서 다른 구성원 초대 • 모든 메인 보드 보기 • 공유 가능 또는 비공개 보드에 초대 받기 • 프로필 수정 • 통신 및 첨부 파일 추가	
시청자	편집 권한 없이 보드만 볼 수 있음	• 계정의 기본 작업 공간에서 모든 보드 보기 • 항목 열기 및 업데이트 읽기	• 새 보드 생성 또는 삭제 • 보드의 콘텐츠, 구조 또는 설정 변경

	(구매한 요금제와 상관없이 시청자를 무제한으로 초대할 수 있음)	• 보드 내에서 검색 또는 필터링 • 공유 가능 또는 비공개 보드에 초대 받기 • 프로필 섹션 수정 • 새로운 시청자 초대 • 보드 보기 개방 • 항목에 할당 받기 • 팀에 추가되기 • 보드를 Excel로 내보내기	• 항목에 업데이트를 추가하거나 다른 사람이 게시한 업데이트에 좋아요 표시 • 항목/보드에 자신과 다른 사람 승인 • 보드 소유자로 지정 받기 • 공유 보드에 게스트 초대하기 • 팀 생성
게스트	공급업체, 고객, 프리랜서 또는 외부 컨설턴트와 같은 조직 외부	• 공유 가능한 보드에 초대 받기 • 구성원의 기능	• 메인 보드 또는 비공개 보드 정보 보기

IP 주소 제한

관리자는 계정에 액세스할 수 있는 허용된 IP 주소 집합을 미리 정의할 수 있습니다. 이를 통해 특정 위치(예: 사무실)에서 참여하거나 특정 VPN을 사용하는 사용자와 같은 특정 컨텍스트의 사용자에 대한 계정 액세스를 제한할 수 있습니다. 허용 목록의 주소와 일치하지 않는 IP 주소로 로그인을 시도하는 모든 사용자는 오류 메시지를 받고 계속 진행할 수 없습니다.
이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.

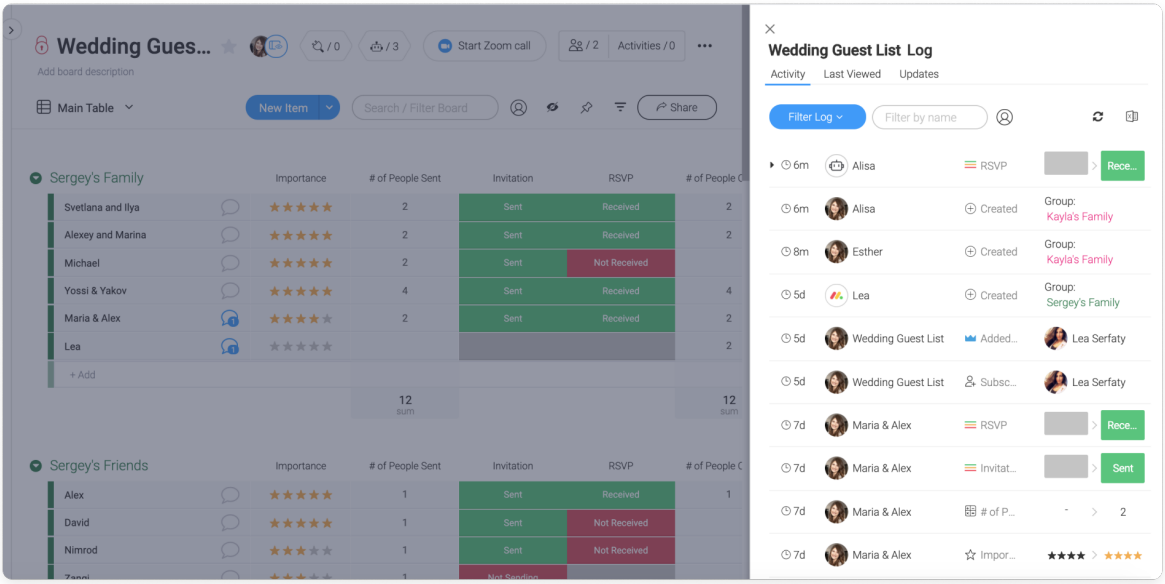


로그

활동 로그

활동 로그에는 두 가지 유형이 있습니다.

1. **보드 활동 로그는** 변경된 날짜, 상태, 그룹 간 이동, 자동화 및 권한을 포함하여 보드의 모든 과거 활동을 하나의 목록에 표시합니다. 보드 활동 로그에 표시되는 정보는 계층에 따라 다릅니다. 기본 플랜에는 지난 주의 활동만 포함됩니다. 표준 플랜은 6개월 동안 활동 데이터를 유지합니다. 프로 및 엔터프라이즈 플랜은 최대 1년까지 유지됩니다.



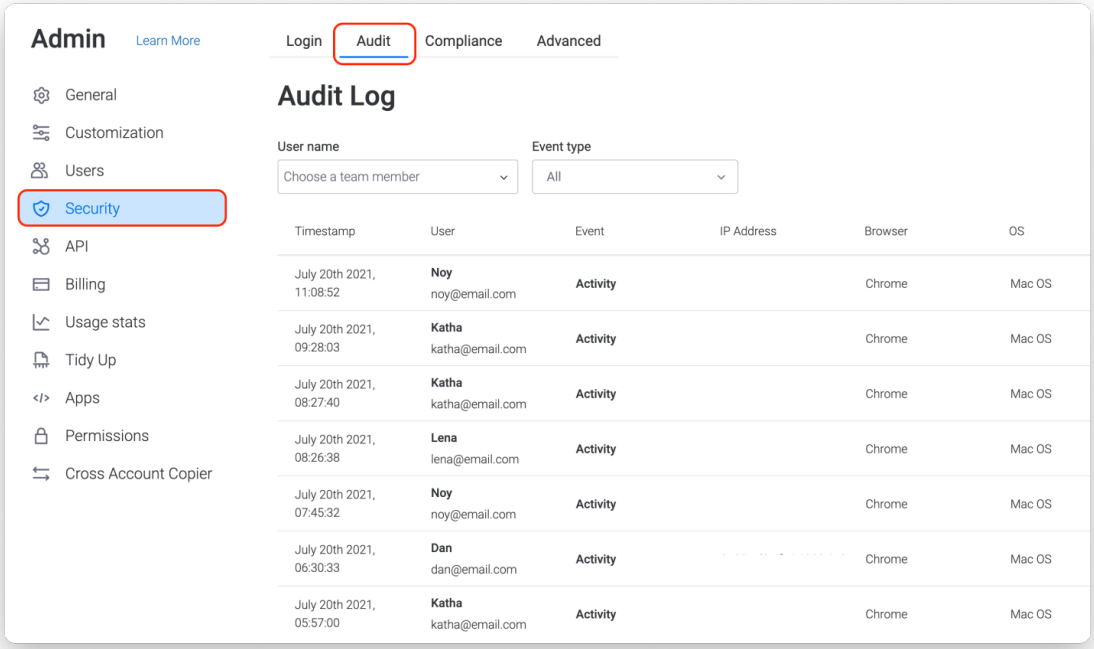
2. **항목 활동 로그는** 개별 항목에 대한 모든 업데이트를 추적합니다. 항목 활동 로그에서 해당 항목의 업데이트에 대한 전체 기록과 정확히 발생한 시간을 볼 수 있습니다. 모든 업데이트는 최신 항목부터 가장 오래된 항목으로 구성됩니다. 모든 업데이트에 대해 경고 알림을 설정할 수 있습니다.

버튼 클릭으로 항목 활동 로그 또는 보드 활동 로그를 Excel로 쉽게 내보낼 수 있습니다.

감사 로그

감사 로그는 계정 관리자에게 모든 계정 보안 관련 활동에 대한 자세한 보고서를 제공합니다. 이 섹션에서는 사용자가 마지막으로 계정에 로그인 및 로그아웃한 시간, 장치 및 세션의 IP 주소를 볼 수 있습니다. 이렇게 하면 의심스러운 활동을 모니터링하고 필요한 경우 패닉 모드를 활성화할 수 있습니다.

로그는 또한 실패한 로그인, 다운로드된 첨부 파일 및 내보낸 보드 데이터와 같은 잠재적으로 취약한 이벤트를 표시합니다. 이 기능은 엔터프라이즈 플랜 고객에게만 제공됩니다.



상호 운용성 및 이식성

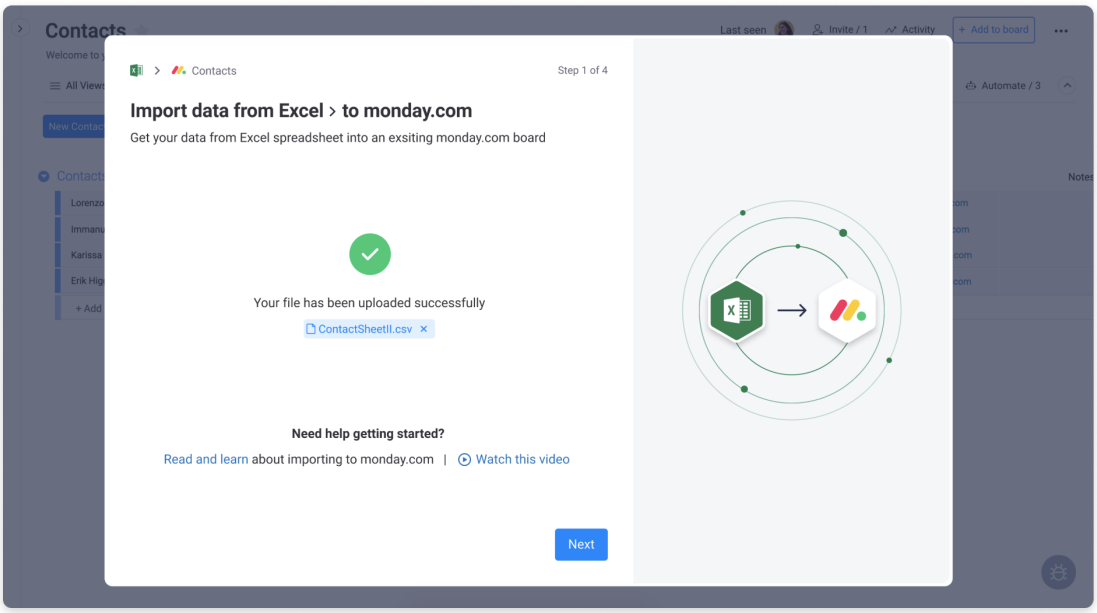
통합

monday.com은 다양한 다른 소프트웨어 솔루션과의 통합을 지원하여 맞춤형 워크플로를 생성합니다. 한 곳에서 모든 팀의 작업을 관리하기 위해 이미 사용하고 있는 도구와 monday.com을 연결할 수 있습니다.
통합은 선택 사항이며 관리자 패널을 통해 비활성화할 수 있습니다.

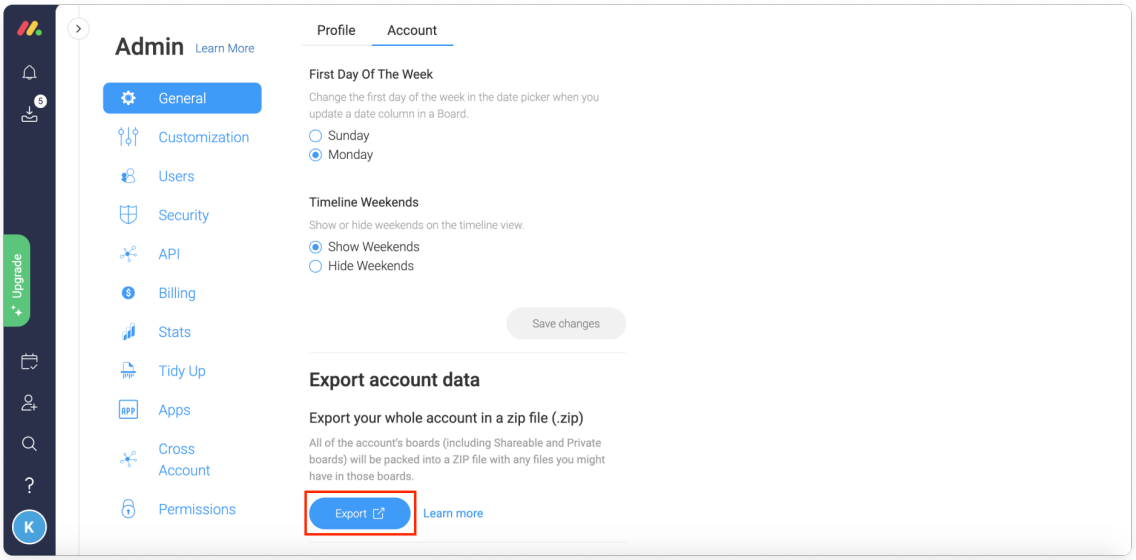
엑셀 가져오기 및 내보내기

monday.com은 고객에게 두 가지 데이터 관리 기능을 제공합니다.

1. Excel 스프레드시트의 데이터를 monday.com 보드(신규 또는 기존)로 변환합니다.



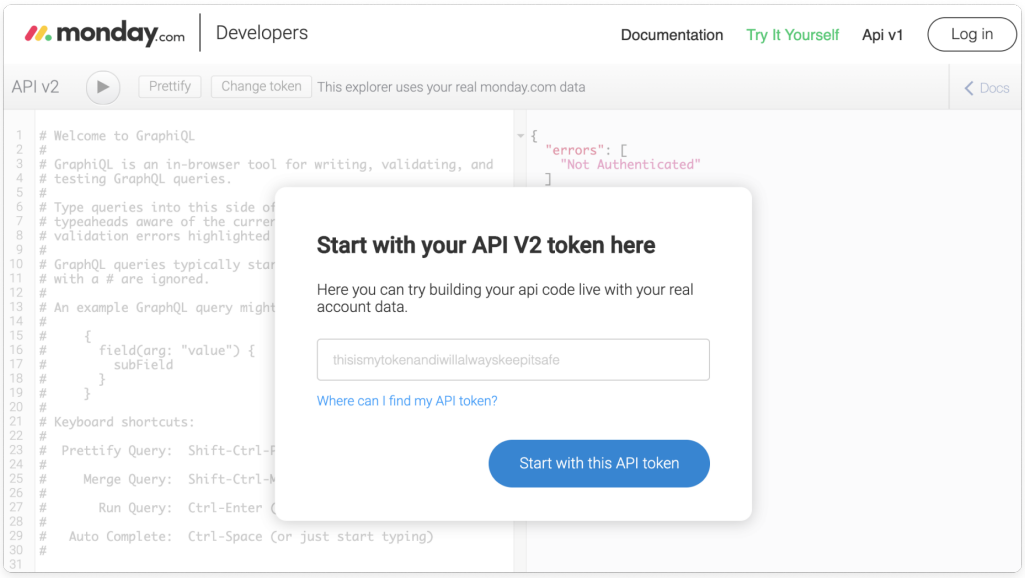
2. monday.com에서 데이터 내보내기:
    a. 보드를 Excel로 내보냅니다.
    b. 관리자 패널을 통해 전체 계정의 데이터를 내보냅니다. 이는 Excel 시트와 계정에 업로드된 파일이 포함된 zip 아카이브로 내보내집니다.



API

monday.com은 GraphQL API를 제공합니다. 이것은 monday 앱 프레임워크의 일부이며 개발자가 monday.com 계정 내의 데이터에 프로그래밍 방식으로 액세스하고 업데이트할 수 있도록 합니다. API 사용 사례는 다음과 같습니다:

- monday.com 대시보드 내에서 사용자 정의 보고서 렌더링을 위한 보드 데이터 액세스
- 다른 시스템에서 레코드를 생성하면 보드에 새 항목 생성
- 프로그래밍 방식으로 다른 소스에서 데이터 가져오기



관리자 패널

관리자 패널에서 계정 관리자는 보안 설정, 계정 사용자, 계정을 사용자 지정하기, 청구 등을 포함하여 모든 것을 관리할 수 있습니다.

승인된 도메인

관리자는 두 가지 설정 중에서 선택할 수 있습니다:

1. 관리자만 모든 이메일 도메인에서 구성원과 시청자를 계정에 초대할 수 있습니다.
2. 관리자는 사용자가 계정에 가입할 수 있는 하나의 이메일 도메인을 결정합니다.

이메일 도메인 차단

관리자는 사용자가 특정 이메일 도메인에서 새 monday.com 계정을 생성하지 못하도록 할 수 있습니다. 이 기능은 동일한 조직, 특히 여러 회사 도메인을 소유한 계정에서 중복된 monday.com

계정을 피하는 데 유용합니다. 이는 기업 데이터 거버넌스 규칙 준수를 유지하는 데 영향을 미칠 수 있습니다.
새 계정 생성을 차단하기 위해 검토 및 소유권을 확인할 수 있도록 이메일 도메인을 monday.com 서비스에 제출할 수 있습니다. 이들은 메인 조직의 계정에 온보딩할 계정 관리자에게 연결됩니다.
이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.

패닉 모드

패닉 모드를 활성화하면 계정이 일시적으로 차단됩니다. 계정 관리자가 고객 성공 팀에 요청을 보낼 때까지 아무도 액세스할 수 없습니다. 이 기능은 팀 구성원의 로그인 자격 증명 중 하나가 손상된 경우 중요합니다.
이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.

세션 관리

관리자 패널의 보안 섹션에서 관리자는 세션 탭을 클릭하여 모든 사용자의 세션 데이터를 보고 모든 세션을 제어 및 재설정할 수 있습니다.
이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.

API 토큰 생성

관리자만 자신의 계정에서 개인 GraphQL API 토큰을 생성할 수 있는 권한을 부여할 수 있습니다(모든 사람에게 또는 관리자에게 만 부여하거나, 아무에게도 부여하지 않거나). 이렇게 하면 사용자가 API 토큰을 생성하여 실수로 제삼자의 도구와 공유하거나 공개 저장소로 푸시하고 계정의 민감한 데이터를 노출하여 공개하는 것을 방지할 수 있습니다. 토큰을 생성할 수 없는 사용자에게는 경고가 표시됩니다.
이 기능은 엔터프라이즈 플랜 고객만 사용할 수 있습니다.

콘텐츠 디렉토리

콘텐츠 디렉토리에서 계정에 있는 모든 작업 공간, 보드, 대시보드 및 워크독스의 개요를 찾을 수 있습니다. 또한 이러한 각 기능에 대해 소유자, 구독자, 생성 날짜, 마지막 업데이트 날짜 및 나머지 계정 구성원이 공개적으로 사용할 수 있는지 여부를 볼 수 있습니다.

* 이 백서에는 관리자 패널을 통해 관리되는 전체 기능 목록이 포함되어 있지 않습니다. 추가 정보는 지원 문서에서 찾을 수 있습니다.
계정 관리자가 관리하는 추가 기능은 로그인, 이중 인증, SCIM 프로비저닝, 권한, IP 주소 제한, monday 앱, 감사 로그, API 토큰 및 HIPAA 규정 준수 구성과 같은 이 문서의 다양한 장에서 다루어질 것입니다.

4. 애플리케이션 보안

안전한 소프트웨어 개발 수명 주기(S-SDLC)

- monday.com은 OWASP 탑 10 방법론을 사용하여 보안 소프트웨어 개발 수명 주기(S-SDLC)를 위한 보안을 구축합니다.
- 모든 코드는 프로덕션에 배포하기 전에 코드 품질을 보장하기 위해 정적으로 분석(SAST)되고 CI/CD 프로세스의 일부로 피어리뷰를 거칩니다.
- 동적 응용 프로그램 보안 테스트(DAST)는 최소한 매주 실행됩니다.
- 당사는 출시된 새로운 기능에 대한 전문적 테스트를 작성하는 데 특히 중점을 두는 반면 이전 기능은 몇 년 동안 전투적 테스트를 거쳤습니다.
- 당사는 배포 중 및 배포 후에 취약점 보완 위해 애플리케이션을 지속적으로 평가하고 모니터링합니다.
- 모든 서버 측 제삼자 라이브러리는 소프트웨어 구성 분석(SCA) 도구를 사용하여 공개된 취약점을 자동으로 확인합니다.

웹 애플리케이션 방화벽(WAF)

웹 애플리케이션 방화벽(WAF)은 알려진 공격을 방어하기 위해 애플리케이션 수준의 트래픽 필터링, 모니터링 및 차단을 위해 마련되었습니다.

취약점 관리

취약점은 개발 백로그에 중앙 집중화되며 서비스 및 고객 데이터의 기밀성, 무결성 및 가용성 영향 평가를 기반으로 분류됩니다. 취약점의 심각도는 종합 취약점 점수 시스템(CVSS)에 의해 결정됩니다. 그런 다음 R&D 부서는 내부 패치 관리 정책에 따라 사전 정의된 심각도 기반 타임프레임 내에서 문제 해결을 실행합니다.

보안 챔피언

내부 보안 챔피언 커뮤니티는 모든 R&D 팀의 개발자로 구성됩니다. 보안 챔피언은 고급 보안 교육을 받고 보안 지침을 제공하며 필요할 때마다 보안 코드 검토를 실행할 자격이 있습니다.

침투 테스트

애플리케이션 침투 테스트는 수동 및 자동 테스트 방법을 포함하는 다른 독립적인 제삼자에 의해 매년 실행됩니다.

또한 내부 애플리케이션 보안팀은 내부 보안 메커니즘과 아키텍처에 대한 깊은 이해가 필요한 다양한 기능에 대해 정기적으로 보안 감사 및 침투 테스트를 실행합니다.

외부 및 내부 침투 테스트의 일환으로 네트워크 스캐닝 도구가 프로덕션 서버에 사용됩니다.

버그 바운티 프로그램

monday.com은 HackerOne에서 내부적으로 관리되는 비공개 버그 바운티 프로그램을 유지 관리하여 전 세계의 보안 연구원이 윤리적이고 책임감 있게 보안 취약점을 연구하고 보안팀에 공개할 수 있도록 합니다. 특정 기능은 보안 커뮤니티 연구와 이러한 영역에 대한 노력에 더욱 집중할 수 있도록 HackerOne에서 제공하는 특별 프로모션을 받습니다.

프로그램의 일환으로 당사는 해커를 위한 명예의 전당 점수판을 유지 관리합니다.

---

5. IT 보안

엔드포인트 보안

모든 직원 워크스테이션은 악성코드 탐지 및 검역을 위한 중앙 관리형 EDR 솔루션으로 보호됩니다.
당사의 EDR 솔루션은 연중무휴 24시간 관리되는 SOC 팀에 의해 지속적으로 모니터링됩니다.
모든 워크스테이션은 FileVault/BitLocker를 사용하여 암호화되어 암호로 보호되며 화면 제한 시간이 10분으로 설정됩니다.
또한 장치 관리자를 통해 패치를 적용하고 원격으로 컴퓨터를 지울 수 있습니다.

비밀번호 정책

당사의 내부 비밀번호 정책은 비밀번호는 최소 12자 이상이어야 하며 다음을 포함해야 합니다:

1. 대문자
2. 소문자
3. 숫자
4. 기호

엔터프라이즈 비밀번호 관리 솔루션이 사용되고, 기본 비밀번호는 정기적으로 변경되며, 반면 비밀번호 재사용 및 일반 비밀번호는 기술적으로 허용되지 않으며, 암호는 120일 후에 만료됩니다.

ID 및 액세스 관리

시스템에 대한 액세스는 HR의 지시에 따라 알 필요 및 최소 권한 원칙에 따라 엔터프라이즈 ID 제공자(IdP) 솔루션을 통한 역할에 따라 IT 팀에서 부여합니다.
사용자 액세스는 고용 변경 또는 고용 종료 후 최대 24시간 이내에 수정됩니다. 또한 분기별 사용자 액세스 심사를 통해 액세스 권한의 적정성을 확인하고 있습니다. 더 이상 필요하지 않은 액세스는 제거되고 문서화됩니다.

이메일 보호

monday.com은 제삼자 메일 릴레이를 사용하여 보호되는 Google Workspace를 이메일 제공업체로 사용합니다. DMARC 및 SPF도 사용합니다. 직원들은 피싱 방지 모범 사례에 대해 지속적으로 교육을 받고 정기적으로 테스트를 실행합니다.

무선 액세스 포인트

monday.com은 업계 표준 기술을 사용하여 본사의 무선 통신을 안전하게 보호합니다. 당사는 다른 도구들 중에서 WPA2 엔터프라이즈를 사용하여 네트워크 전반에 걸쳐 적시에 프로비저닝 해제 및 부인 방지를 보장하고 악성 AP 모니터링을 시행합니다.

6. 운영 보안

고객 데이터 액세스

monday.com은 고객이 monday.com 서비스에 제출하는 모든 데이터를 "블랙박스"와 같이 취급하며 전적으로 고객을 대신하여 처리합니다. 이는 일반적으로 monday.com 서비스의 성능을 이유로 고객 데이터에 액세스하지 않으며 제출된 모든 고객 데이터를 최고 수준의 민감도와 기밀로 취급한다는 것을 의미합니다.
monday.com의 고객 데이터 액세스는 사례별로 서비스 약관 또는 고객과의 각 계약에 따라 제한됩니다.

인적 자원

배경 점검

당사의 본사는 배경 점검이 관습적이지 않으며 법에 따라 제한되는 이스라엘에 있습니다. 당사가 실행하는 점검에는 작업 기록 및 이전 직속 관리자와의 참조 통화가 포함됩니다.

고용 계약

monday.com의 모든 고용 계약에는 기밀 조항과 특정 의무 및 약속 위반 시 즉시 종료할 수 있는 조항이 포함되어 있습니다.
또한 monday.com은 채용부터 퇴사까지 고용 기간 동안 필요한 보안 활동과 책임을 정의하는 HR 보안 정책을 유지합니다.

사용 제한

monday.com은 보안팀과 보다 광범위한 보안 포럼에서 사용 제한 정책을 매년 검토하고 유지 관리합니다. 직원은 온보딩 시 또는 정책의 중대한 변경이 있을 경우 정책에 서명해야 합니다.

교육 및 인식

monday.com 직원은 초기 온보딩 프로세스의 일부로, 그 후 최소 1년에 한 번 실행해야 하는 정보 보안 및 개인정보 보호 의무에 관한 교육을 받습니다. 교육에는 튜토리얼과 서면 작업이 포함되며 보안팀에서 모니터링합니다.
직원의 인식을 더욱 높이기 위해 분기별 보안 및 개인정보 보호 주간이 실시됩니다.
또한 필요에 따라 전용 교육 세션을 실시합니다(예: 개발자는 보안 코딩 교육을 받습니다).

근로 계약 종료

사용자 액세스는 회사 장비 반환과 함께 고용 변경 또는 고용 종료 후 최대 24시간 이내에 수정됩니다. 액세스 권한의 적정성을 확인하기 위해 분기별로 사용자 액세스 검토를 실행합니다.

레드팀 평가

일년에 두 번 내부 침투 테스트, 인프라 공격 및 가상 위반 시뮬레이션을 포함하여 방어 태세에 대한 레드팀 평가를 실행합니다. 레드팀 평가는 정교한 첨단 공격 기술을 사용하여 잠재적인 보안 위험 및 취약성에 대한 고유한 가시성을 제공하는 공격적이면서도 방어적이며 앞서가는 제삼자 보안 컨설팅 회사에서 실행합니다.

거버넌스 및 위험 관리

monday.com은 monday.com 시스템 내의 취약성을 사전에 식별하고 회사 운영에 대한 새로운 것과 드러나는 위협을 평가하기 위한 지속적인 위험 관리 프로세스를 유지 관리합니다. monday.com은 매년 실행되는 ISO 27001 인증의 일환으로 위험 평가를 받습니다.

사고 대응 및 관리

monday.com의 사고 대응 계획(IRP)은 보안 및 개인정보 보호 사고를 감지하고 관련 담당자에게 전달, 소통(내부 및 외부), 완화 및 사후 분석을 위한 지침을 제시합니다.
monday.com의 사고 대응 팀(IRT)은 보안, R&D, 법무 부서 대표, 다양한 사례별 팀 대표, 그리고 필요한 경우 제삼자 사고 대응 회사로 구성됩니다.

알림

데이터 사고를 인지한 후 당사의 데이터 처리 부록("데이터 사고 관리 및 알림") 섹션 7에 따라 monday.com은 해당 고객에게 부당한 지연 없이 바로 알릴 것입니다.
영향을 받는 고객은 침해의 성격, monday.com이 인지하고 있는 유해한 영향, monday.com이 취한 조치, 알림 시점에 사고를 시정하거나 완화할 계획에 대해 알림을 받습니다.

재해 복구 및 비즈니스 연속성

monday.com은 물리적 사무실(프로덕션 인프라의 일부가 보관되지 않는 장소)에 영향을 미치는 재해를 처리하기 위해 ISO 27001에 따라 비즈니스 연속성 플랜을 유지 관리합니다.
또한 전용 DR 위치에서 서비스의 핵심 기능 복원을 포함하여 프로덕션 환경에 영향을 미치는 재해를 처리하기 위한 재해 복구 계획(DRP)을 유지 관리합니다. 테스트는 적어도 1년에 두 번 실시됩니다. monday.com의 DR 테스트는 연습, 모의 재해 또는 구성 요소 테스트의 형태로 이루어질 것입니다.

데이터 보존 및 폐기

데이터 보존

monday.com은 개인정보 보호정책에 설명된 목적을 달성하는 데 필요한 기간에 monday.com이 통제하는 귀하의 정보를 보유합니다. monday.com이 고객을 대신하여 처리하는 데이터는 서비스 약관, 데이터 처리 부록 및 해당 고객과의 기타 상업적 계약에 따라 유지됩니다.

데이터 삭제

monday.com 고객은 제출한 데이터를 완전히 제어할 수 있으며 서비스의 사용자 인터페이스를 통해 사용 가능한 수단으로 항상 데이터를 수정, 내보내기 또는 삭제할 수 있습니다.
구독이 종료되거나 만료되면 고객은 계정 폐쇄 절차의 일부로 데이터 삭제를 요청할 수 있습니다. 고객 데이터는 요청 후 90일 이내에 삭제되며 여기에는 롤백을 허용하는 30일과 삭제 프로세스를 진행하기 위한 추가 60일이 포함됩니다.
또는 고객은 계정 데이터를 플랫폼에 유지하는 것을 선택할 수 있으며, 이 경우 당사는 계속 보유할 수 있지만 당사의 재량에 따라 언제든지 삭제할 수도 있습니다.

데이터 파기

당사 서비스는 AWS에서 호스팅되며 특정 데이터는 GCP에 백업됩니다. 두 클라우드 컴퓨팅 제공업체 모두 다중 테넌트 환경에서 민감한 데이터를 안전하게 저장할 수 있도록 독점 데이터 배포 및 삭제 전략을 구현합니다. 스토리지 미디어 폐기는 NIST 800-88에 설명된 기술을 사용하여 앞서 언급한 공급업체에 의해 실행됩니다.

모니터링 및 로그

monday.com은 네트워크 침입 감지 시스템(NIDS), 엣지 로케이션의 트래픽 로그, 이벤트 추적 및 감사를 위한 애플리케이션 수준 로깅, 액세스 및 고도의 운영 감사를 위한 시스템 수준 로깅을 사용하여 네트워크 로그를 수집하고 모니터링합니다. 로그는 보안 정보 및 이벤트 관리(SIEM) 솔루션으로 스트리밍되며 관리되는 SOC 팀에서 지속적으로(연중무휴 24시간) 모니터링합니다.

공급망 관리

하위 프로세서

monday.com은 데이터 보안 및 개인정보 보호와 관련하여 업계 표준에 따라 하위 프로세서(글로벌 데이터 영역 및 EU 데이터 영역 모두)를 유지하고 두 영역을 하위 프로세서 선택 과정에서 중요하게 다루어집니다. 당사는 다른 조치 중에서 데이터 처리 부록과 기타 관련 문서 및 보호 장치가 모든 하위 프로세서에 적용되도록 하고 개인정보 보호, 법률 및 정보 보안 평가와 설문 기반 감사를 모두

준수하며 업계 표준 및 규제 요구 사항을 준수합니다. 당사의 하위 프로세서에 대한 평가는 최소한 매년 실행됩니다.

공급업체 관리

monday.com은 당사가 사용하는 서비스와 소프트웨어 모두에 대한 중앙 저장소 자산 관리 프로그램을 가동합니다. 저장소 자산은 보안, 법률, 개인정보 보호 및 조달 팀에서 지속적으로 유지 관리하며 승인 프로세스는 모든 직원에게 전달됩니다.
서비스 또는 소프트웨어의 사용 및 갱신 시작 시, 다양한 팀이 액세스할 수 있는 가장 높은 데이터 민감도 수준에 따라 우리와 협력하는 공급업체를 분류하여 적절한 위험 수준을 결정하고 산업 표준 및 규제 요구 사항에 따라 검토합니다.

물리적 보안

monday.com 사무실

monday.com 사무실의 물리적 IT 자산은 랩톱 및 사무실 네트워크 장치로 제한됩니다. 사무실 네트워크 장치는 연중무휴 24시간, CCTV 모니터링, 환경 제어 서버실에서 암호로 잠겨 보호됩니다. 사무실에 대한 물리적 접근은 생체 인식을 통해 제어됩니다. 방문자는 사무실에 입장할 때 로그인되며 사무실에 머무는 동안 monday.com 직원이 항상 에스코트해야 합니다. 모든 직원은 의심스러운 활동, 구내 무단 액세스, 도난 또는 분실물 사고를 보고해야 합니다.

데이터 센터 보안

monday.com은 AWS와 GCP의 세계적 수준의 물리적 및 환경적 보안 조치에 의존하여 매우 탄력적인 인프라를 구축합니다. 이러한 보안 관행에 대한 자세한 내용은 다음 링크를 참조하시기 바랍니다.
https://aws.amazon.com/security/, https://cloud.google.com/security/

---

7. 규정 준수, 개인정보 보호 및 인증

감사 보증 및 규정 준수

monday.com은 여러 산업 표준 규정 준수 프로그램과 당사 서비스가 제공되는 지역의 주요 개인정보 및 데이터 보호 규정에 따라 보안 및 개인정보 보호 프로그램을 개발했습니다.

ISO 27001, 27017, 27018, 27032, and 27701

monday.com은 국제 표준화 기구(ISO)의 국제 표준을 준수하며 그에 따라 정보 보안, 클라우드 서비스 및 개인정보를 관리합니다. 당사는 매년 독립적인 제삼자로부터 감사를 받고 5개의 ISO 인증서를 유지 관리합니다:

- **ISO/IEC 27001:2013**은 정보 보안 관리 시스템(ISMS)에 대한 가장 엄격한 글로벌 보안 표준입니다.
- **ISO/IEC 27018:2014**는 공용 클라우드 컴퓨팅 환경에 대한 ISO/IEC 29100의 개인정보 보호 원칙에 따라 개인 식별 정보(PII) 보호 조치 구현을 위해 일반적으로 허용되는 제어 목표, 제어 수단 및 지침을 설정합니다.
- **ISO/IEC 27017:2015**는 클라우드 서비스 공급자와 클라우드 서비스 고객 모두를 위한 제어 및 구현 지침을 제공합니다. 이는 목적에 적합한 제어를 위해 추가 구현 지침을 제공하여 클라우드 서비스 규정과 사용에 적용 가능한 정보 보안 제어 지침을 제공하는 것입니다.
- **ISO/IEC 27032:2012**는 사이버 보안의 고유한 측면과 다른 보안 도메인, 특히 정보 보안, 네트워크 보안, 인터넷 보안 및 중요 정보 인프라 보호(CIIP)에 대한 종속성을 도출하여 사이버 보안 상태를 개선하기 위한 지침을 제공합니다.
- **ISO/IEC 27701:2019**는 개인정보 관리 시스템(PIMS)을 구축, 구현, 유지 관리 및 지속적으로 개선하기 위한 요구 사항을 지정하고 지침을 제공합니다.

모든 인증은 여기에서 찾을 수 있습니다.

SOC 1, SOC 2, 및 SOC 3

monday.com은 서비스 및 조직 제어를 달성했습니다:

- **SOC 1 유형 II 감사**는 고객의 재무 보고와 관련될 수 있는 통제를 감사합니다.
- **SOC 2 유형 II 감사**는 업계에서 가장 엄격한 보안, 가용성 및 기밀성 표준을 충족하기 위한 당사의 약속을 보여줍니다. 이는 monday.com의 보안 제어가 미국 공인 회계사

협회(AICPA)의 신뢰 서비스 원칙과 기준 및 HIPAA 보안 요구 사항을 준수하는지 확인합니다.

- **SOC 3 보고**는 SOC 2 유형 II 보고서의 짧은 버전이며 공개적으로 사용 가능합니다.

감사는 독립적인 제삼자에 의해 매년 실행되며 매년 4월부터 3월까지의 보고서가 발행됩니다. monday.com의 SOC 보고서는 SOC 1, SOC 2 및 SOC 3 링크에서 찾아 볼 수 있습니다.

클라우드 보안 얼라이언스(CSA)

클라우드 보안 얼라이언스(CSA)는 "클라우드 컴퓨팅 내에서 보안 보증을 제공하기 위한 모범 사례의 사용을 촉진하고 다른 모든 형태의 컴퓨팅을 보호하기 위해 클라우드 컴퓨팅 사용에 대한 교육을 제공"하는 것을 사명으로 하는 비영리 조직입니다. monday.com은 자발적인 CSA STAR인 보안, 신뢰, 보증 및 위험 등록 자체 평가에 참여하여 CSA에서 게시한 모범 사례 준수를 문서화합니다. 완성된 CSA CAIQ인 컨센서스 평가 이니셔티브 설문지는 무료이며 CSA 웹사이트에서 공개적으로 사용할 수 있습니다.

건강 보험 이전 및 책임에 관한 법률(HIPAA)

건강 보험 이전 및 책임에 관한 법률(HIPAA)은 의료 데이터를 보호하도록 설계되었습니다. 병원, 의사 사무실, 건강 보험 또는 보호 건강 정보(PHI)를 취급하는 회사와 같은 조직은 HIPAA를 준수해야 합니다. 이는 이러한 사업체와 협력하며 그들을 대신하여 PHI와 접촉하는 회사에도 적용될 수 있습니다.

monday.com은 엔터프라이즈 플랜 HIPAA 준수 계정 구성을 고객에게 제공하여 그러한 고객이 민감하게 생각하는 의료 정보를 제출할 수 있도록 합니다. 당사의 HIPAA 고객은 HIPAA 데이터를 제출하기 전에 PHI를 보호하고 적절하게 처리하기 위해 업무 제휴 계약(BAA)을 체결해야 합니다.

monday.com 및 GDPR

당사의 글로벌 개인정보 보호 프로그램은 당사의 "북극성" 역할을 하는 세계에서 가장 포괄적이며 가장 강한 데이터 보호 규정과 EU 및 영국 일반 데이터 보호 규정(GDPR)을 기반으로 합니다.

무엇보다도 monday.com의 개인정보 보호 포럼은 개인정보 보호 중심 설계(Privacy-by-Design) 원칙, 데이터 최소화 및 저장 제한, 처리의 합법성 및 공정성, 활동 및 목적에 대한 투명성 등과 같은 GDPR 원칙이 유지되도록 개인 데이터를 사용하는 것과 관련된 다양한 활동을 포함한 조직 전체의 제품 및 프로세스 개발을 지속적으로 모니터링합니다.

개인정보 보호정책

monday.com의 개인정보 보호정책은 데이터 컨트롤러로서 당사가 자체 목적으로 처리하는 개인 데이터와 관련하여 당사의 개인정보 및 데이터 처리 관행을 설명하고 있으며, 다음 링크에서 확인할 수 있습니다.

데이터 처리 부록(DPA)

monday.com의 서비스 약관 및 고객 계약에는 고객을 대신하여 개인 데이터를 보호하고 적절하게 처리하기 위한 데이터 처리 부록이 포함되어 있습니다. 온라인에서 데이터 처리 부록(DPA)을 검토하고 실행할 수 있습니다.

개인 데이터의 국가 간 전송

monday.com은 이스라엘에 본사가 있으며 미국, 영국, 호주 및 브라질에 자회사가 있고 우크라이나 및 과테말라에 지원 팀이 있습니다. 당사의 하위 프로세서는 하위 프로세서 페이지에 자세히 설명된 바와 같이 다양한 국가에 등록되어 있습니다.

당사가 EEA와 영국에서 다른 국가로 개인 데이터를 전송할 때, 유럽위원회가 내린 "적정성 결정"과 같은 GDPR에 따라 제공되는 합법적인 전송 메커니즘(예: 영국과 이스라엘이 EU에서 비롯된 개인 데이터에 적절한 수준의 보호를 제공하는 것으로 간주하는 결정)에 의존하며, EU 표준 계약 조항은 여기와 여기에서 찾을 수 있습니다.

컨트롤러 및 프로세서

GDPR은 개인 데이터 수집 및 처리와 관련하여 데이터 컨트롤러와 데이터 프로세서라는 두 가지 기본 역할을 정의하고 구분합니다. 데이터 컨트롤러는 개인 데이터를 처리하는 수단과 목적을 결정하는 반면 데이터 프로세서는 컨트롤러를 대신하여 데이터를 처리하는 당사자입니다.

- monday.com은 고객, 사용자 및 웹사이트 방문자와 관련된 개인 데이터의 데이터 컨트롤러입니다. 이는 당사의 개인정보 보호정책에 자세히 설명되어 있습니다.
- monday.com은 고객과 사용자가 플랫폼(monday.com 계정 내 보드 및 항목으로)에 제출하는 개인 데이터의 프로세서이며 고객을 대신하여 이 데이터를 처리합니다. 당사는 고객과 체결한 데이터 처리 부록에 따라 처리합니다. 당사가 이 데이터를 처리하는 데 사용하는 제삼자 서비스 제공자는 당사의 "하위 프로세서"입니다.

monday.com 및 CCPA

monday.com은 "서비스 제공자"로서 고객이 중단 없이 monday.com을 계속 사용할 수 있게하고, CCPA에 따라 캘리포니아 소비자의 개인정보를 처리하고 있음을 보장하기 위해 2018년 캘리포니아 소비자 개인정보 보호법(CCPA)의 해당 요구 사항과 전 세계적으로 유사한 규정(예: GDPR) 및 진화하는 업계 표준을 반영한 캘리포니아 법무장관 규정 준수에 최선을 다하고 있습니다.
추가 정보는 여기에서 찾아 볼 수 있습니다.

호주 개인정보 보호법(APA) 및 호주 개인정보 보호 원칙(APP)

호주 개인정보 보호법(APA) 및 호주 개인정보 보호 원칙(APP)은 개인정보를 수집, 처리, 사용 및 공유하기 위한 구조화된 프레임워크를 설정하여 개인이 정보 처리 방식을 더 잘 제어할 수 있도록 합니다. monday.com은 APA 및 APP의 요구 사항을 준수하기 위해 최선을 다하고 있습니다.
추가 정보는 여기에서 찾아 볼 수 있습니다.

내부 감사

당사의 보안, 개인정보 보호, 인프라, R&D, IT, 운영 및 법무 팀은 분기별 보안 및 개인정보 보호 주간을 정하고 사용자 액세스 검토, 방화벽 구성 검토, 클린 데스크 검사, 인식 교육 및 활동 등이 포함된 다양한 감사 활동을 실행합니다.

정부 당국에 공개

monday.com은 당사에 보관된 고객 데이터에 대한 정부 당국의 부당한 액세스를 허용하지 않습니다. 당사는 미국 또는 기타 국가에서 당국으로부터 고객 데이터 공개 요청을 거의 받지 않습니다. 지난 몇 년 동안 이러한 요청을 받은 몇 가지 사례는 범위가 제한적이었으며 요청했던 해당 데이터(예: 특정 계정과 관련된 불법 활동이 의심되는 데이터)는 매우 합법적인 근거를 가지고 다루었습니다.
요청이 유효하고 보증되는지 확인하기 위해 법률 및 개인정보 보호 팀에서 요청을 검토한 후 법에 따라 엄격하게 필요한 데이터로 제한하여 공개됩니다. 공개가 금지되거나 잠재적 위험으로 인해

불가능하지 않는 한, 공개하기 전에 고객에게 알리기 위해 상업적으로 합당한 노력을 기울입니다.[3] 당사는 또한 FISA의 702항을 포함하여 GDPR 또는 영국 GDPR에 따라 보호되는 개인 데이터와 관련된 대량 감시 요청에 대해 적용 가능한 법률에 따라 상업적으로 합당한 노력을 기울일 것을 약속합니다.

개인정보 보호팀 및 DPO

monday.com은 이스라엘 최고의 개인정보 보호 컨설팅 업체인 PrivacyTeam의 보호를 받고 있으며 PrivacyTeam과 협력하여 고객 데이터와 개인정보를 보호하기 위해 노력하고 있습니다. 추가 정보는 여기에서 찾을 수 있습니다.

monday.com은 monday.com의 지속적인 개인정보 규정 준수를 모니터링 및 조언하고 데이터 주체 및 감독 기관의 개인정보 문제에 대한 연락 창구 역할을 하기 위해 PrivacyTeam의 개인정보 보호에 베테랑인 미스터 아네르 라비노비츠(Mr. Aner Rabinovitz)를 데이터 보호 책임자로 임명했습니다.

---

[3] 추가 정보는 당사 개인정보 보호정책의 섹션 4("데이터 공유")에서 확인할 수 있습니다.

8. 에필로그

이 백서는 보안 및 개인정보 보호에 대한 monday.com의 접근 방식에 대한 광범위한 개요를 제공합니다. 물론 이러한 주제의 복잡성을 고려할 때 추가 질문이 있을 수 있습니다.
보안 신뢰 센터 및 법률 포털에서 추가 정보를 찾아 볼 수 있습니다.
monday.com의 정보 보안 또는 개인정보 보호 상태에 대한 추가 설명은 support@monday.com을 통해 연중무휴 24시간 제공되는 일반 지원 외에도 security@monday.com 또는 dpo@monday.com을 통해 당사에 문의할 수 있습니다.
보안 문제 또는 취약점을 보고하시겠습니까? security@monday.com으로 이메일을 보내거나 https://monday.com/security/form/에서 HackerOne 양식을 통해 보고하세요.

면책 고지: 이 버전은 오로지 편의를 위해 제공되는 영어 원본의 번역문입니다. 영어 원본이 공식적이고 법적 구속력이 있는 버전이며, 불일치할 경우 영어 원본이 우선합니다.