



Monday.com'da Güvenlik & Gizlilik

 **monday.com**

Sıkça Sorulan Soruların Cevapları

İhtiyacınız olan cevapları alın

Monday.com'un güvenlik & gizlilik SSS bölümüne hoş geldiniz. Bu belgede, uygulamalarımızın ve altyapımızın güvenliği ile ilgili sık sorulan önemli soruların yanıtları ve API'mız ve olay hazırlığımız ile ilgili ayrıntılar bulacaksınız. Bu belge en sık yanıtlanan soruların yanıtları içerse de, ek sorularınız veya açıklama talepleriniz varsa, lütfen support@monday.com adresinden 24/7/365 destek ekibimize iletişime geçin.

İçindekiler

Kurumsal Güvenlik	1
Uygulama Güvenliği	4
Altyapı Güvenliği	7
Olay Hazırlığı	9
Entegrasyon Seçenekleri	9

Kurumsal Güvenlik

1 S: Monday.com'un resmi bir bilgi güvenliği programı var mı?

C: Evet. Program, monday.com için geçerli yerel ve uluslararası yürürlükteki yasaları, standartları ve yönetmelikleri dikkate alır ve monday.com hizmetini ve müşterilerinin verilerini korumak için tasarladığımız önlemleri ve kontrolleri tanımlar.

Program ISO 27001'e dayanmaktadır ve iştirakleri, çalışanları, yüklenicileri, taşeronlar, ortakları ve monday.com'u oluşturan, koruyan, depolayan, erişen, süreçler veya ileten herkes de dahil olmak üzere tüm monday.com organizasyonunu veya monday.com tarafından sağlanan hizmetin performansı ile bağlantılı olarak kullanıcılarının bilgileri kapsar.

2 S: Monday.com, burada belirtilen tarih itibariyle hangi Güvenlik ve Gizlilik ile ilgili yönetmelikler, standartlar ve sertifikalara uygundur?

C: Aşağıdaki sertifikalara, raporlara ve uyumluluk programlarına sahibiz:



Tüm sertifikalarımızı [burada](#) bulabilirsiniz.

3 S: Monday.com'da özel güvenlik personeli var mı?

C: Evet. Güvenlik çabalarımız, Altyapı, & Ar-Ge, Operasyonlar ve BT Ekiplerinden temsilcilerden oluşan Güvenlik Ekibimiz ve daha geniş Güvenlik Forumu tarafından yönlendirilmekte ve izlenmektedir.

4 S: Monday.com'un gizlilik yasaları/yönetmeliklerine ve yönetmeliklere ilişkin güncellemeleri ele almak için resmi bir süreci var mı?

C: Yasal, Gizlilik ve Güvenlik Ekiplerimizin temsilcilerinden oluşan ve DPO liderliğindeki Gizlilik Forumumuz, geçerli gizlilik yasaları/yönetmeliklerine ve düzenleyici rehberliğe yönelik güncellemeleri sürekli olarak izler. Forum, "Tasarımla Gizlilik" yaklaşımımızı sürdürmekten ve yeni veya önerilen ürün gelişmeleri ve diğer girişimlerin veri korunmasından sorumludur.

5 S: Monday.com PCI-DSS uyumlu mu?

C: Monday.com, PCI-DSS sertifikalı bir fatura işlemcisinin hizmetlerini kullanır; bu nedenle, üçüncü taraf fatura işlemcimiz aracılığıyla ödenen kredi kartı ödemeleri PCI-DSS uyumludur. Monday.com'un hizmeti PCI-DSS sertifikasına

sahip değildir ve buna bağı olarak hizmetiyle ilgili fatura bilgilerini işlemez, Böylece PCI-DSS verileri hizmetimizde depolanmaz.

6 S: Monday.com'un resmi bir bilgi güvenliği programı var mı?

A: Evet. İlk işe alım sürecimizin bir parçası olarak ve sürekli olarak (en azından yıllık olarak), çalışanlarımız ilgili bilgi güvenliği yükümlülüklerine ilişkin eğitim alırlar.

Üç Aylık Güvenlik & Gizlilik Haftaları, tüm şirket çalışanları arasında farkındalığı daha da artırmak için yürütülmektedir. Buna ek olarak, geliştiriciler, en az yıllık olarak güvenlikle ilgili geliştirme konusunda güncel kalmaları için periyodik güvenlik eğitime tabi tutulur.

7 S: Monday.com'un bilgi güvenliği politikaları ne sıklıkta inceleniyor?

C: Bilgi güvenliği politikalarımız en az yıllık olarak veya hizmetimizde veya güvenlik ve gizlilik duruşumuzda önemli bir değişiklik üzerine gözden geçirilir.

8 S: Monday.com'un Gizlilik Bildirimi/Politikası var mı?

C: Evet, Gizlilik Politikamızı [burada](#) bulabilirsiniz.

9 S: Monday.com, bizimle paylaştığınız kişisel verilere erişimi olacak herhangi bir işlemci/alt işlemciyi devreye sokuyor mu?

C: Evet, hizmetimizin performansı için birkaç alt işlemci kullanıyoruz. Alt işlemcilerimizin listesi (verileri sizin adınıza işleyen), konumları ve bize sağladıkları hizmet türü dahil olmak üzere [burada](#) mevcuttur.

Alt işlemciler listemizde yapılan değişikliklerle ilgili e-posta bildirimleri almak için yukarıdaki bağlantıdan da abone olabilirsiniz.

Uygulama Güvenliđi

10 S: Monday.com ne tür veriler toplar?

C: Yeni bir hesap oluşturulduktan sonra, tarafınızdan bize sağlanan kişisel verilerinizi (örneğin: kullanıcının tam adı, e-posta adresi ve telefon numarası) saklarız.

Monday.com hizmetini kullanmaya başladığınızda, tarafımızdan saklanan veriler, hizmetin kullanımınıza ve veri türüne (metin, dosyalar vb.), ve ayrıca siz ve hizmette oturum açan diğer yetkili kullanıcıların monday.com'a göndermeye karar verdikleri verilerden oluşur.

Daha fazla bilgi [Gizlilik Politikamızda bulunabilir](#).

11 S: Monday.com, kullanıcılarının monday.com hizmetine erişimini nasıl güvence altına almıştır?

C: Monday.com'a erişim aşağıdaki kimlik doğrulama yöntemleri ile gerçekleştirilir:

- Kimlik bilgileri: kullanıcı adı (genellikle e-posta adresiniz) ve şifre;
- Ayrıca Google SSO (yalnızca Pro & Enterprise planı için) ve Okta, OneLogin ve özel SAML 2.0 (yalnızca Kurumsal plan için) gibi harici kimlik sağlayıcılarının kullanımını da destekliyoruz;
- Buna ek olarak, bir metin mesajı veya kimlik doğrulayıcı uygulama aracılığıyla iki faktörlü kimlik doğrulama (2FA) hesap yöneticileri tarafından isteğe bağlı olarak etkinleştirilebilir.

12 S: Monday.com parola politikalarının yapılandırılmasını destekliyor mu?

C: Yöneticilere hesapları için iki parola güç ayarı seçeneđi sunuyoruz:

Yinelenen veya ardışık karakterlere izin verilmeyen en az 8 karakter; veya tekrarlayan veya ardışık karakterlere izin verilmeyen en az 8 karakter ve en az bir basamak (123), bir küçük harf (abc) ve bir büyük harf (ABC).

13 S: Monday.com müşterilerinin verileri şifrelenir mi? Verileri şifrelemek için hangi metodolojiler kullanılır?

C: Evet, monday.com müşteri verilerini şifrelemek için aşağıdaki yöntemleri kullanır:

- Geri kalan veriler AES-256 kullanılarak şifrelenir.
- Açık ağlar üzerinden aktarılan veriler TLS 1.3 (en az TLS 1.2) kullanılarak şifrelenir.
- Kullanıcı parolaları hashlenerek şifrelenir.

14 S: Monday.com kodunun güvenli bir şekilde geliştirildiğinden nasıl emin olur?

C: Yazılım geliştirme yaşam döngümüzde güvenlik sağlamak için OWASP Top 10 ve CVSS standartlarını kullanıyoruz. Geliştiricilerimiz tarafından yazılan tüm kodlar statik olarak analiz edilir ve dağıtımından önce kod kalitesini sağlamak için ekran gözden geçirilir. Dağıtım sırasında ve sonrasında güvenlik açıkları için uygulamamızı sürekli olarak değerlendirir ve izleriz

15 S: Monday.com uygulama güvenliği testi yapar mı?

C: Evet, uygulama penetrasyon testi, değişken bağımsız bir üçüncü taraf tarafından yıllık bazda gerçekleştirilir. Buna ek olarak, bir hata ayıklama programı sürdürüyoruz ve DAST taramaları en az iki haftalık bazda gerçekleştiriliyor.

16 S: Monday.com verilerimi ne kadar süre saklıyor? Hizmeti kullanmayı bırakırsam ne olur?

C: Monday.com müşterileri yüklenen verilerinin tam kontrolünü elinde tutar ve monday.com'un kullanıcı arayüzü üzerinden kendilerine sunulan araçları kullanarak abonelik dönemi boyunca her zaman değiştirebilir veya silebilirler. Monday.com'un yönetim paneli üzerinden yapılan hesap kapatma prosedürünün bir parçası olarak verilerinizin silinmesini talep edebilirsiniz. Gönderdiğiniz tüm verileriniz daha sonra 90 gün içinde silinir; bu, geri alma için 30 günlük bir süre ve veri tabanlarımızdan ve alt işlemcilerimizin veri tabanlarındaki verileri silmek için 60 gün ilave gün içerir.

Alternatif olarak, hesabınızı kapattıktan ve aboneliğinizi iptal ettikten sonra bile hesabınızın verilerini saklayabilirsiniz. Bu durumda mevcut politikamız, belirli bir süre taahhüt edilmeksizin tutmaktır. Bu gibi durumlarda, bildirimde bulunarak veya bildirmeden silebiliriz.

Hesabınızdaki verileri istediğiniz zaman iki biçimde dışa aktarabileceğinizi lütfen unutmayın:

- Panolar Excel'e aktarılabilir;
- Hesabın tüm verileri yönetici panelinden Excel sayfaları ve hesaba yüklenen dosyalar içeren bir zip arşivine aktarılabilir (yalnızca yöneticilerle sınırlıdır).

17 S: Monday.com platformda kullanıcı etkinliğinin denetim günlüklerini sağlıyor mu?

C: Evet, günlükler iki şekilde sağlanır:

- Kurul düzeyinde etkinlik, [etkinlik günlüğünde](#) görüntülenebilir.
- Başarılı/başarısız oturum açma girişimleri [Denetim Günlüğü'nde](#) görüntülenebilir.

18 S: Monday.com uygulamasında hangi yetkilendirme rolleri mevcuttur?

C: Hizmetimizdeki roller yöneticiler, üyeler, misafirler ve izleyicileri içerir. [Bu makalede](#) daha fazla ayrıntı bulabilirsiniz.

Buna ek olarak, hizmetimizdeki erişim kontrolü şu özelliklerden yararlanılarak sağlanır: [Çalışma alanları](#), [pano türleri](#), [pano düzeyi izinler](#) ve [sütun düzeyinde izinler](#).

19 S: Monday.com'un dış tarafların güvenlik açıklarını bildirmesi için kolayca keşfedilebilir bir yolu var mı?

C: Evet, güvenlik açıkları security@monday.com adresine veya [buradaki](#) HackerOne güvenlik açığı gönderme formumuz aracılığıyla bildirilebilir.

Altyapı Güvenliđi

20 S: Monday.com'un veri merkezleri nerede bulunur?

C: Monday.com tamamen bulut tabanlı bir hizmettir. Hizmetimiz Kuzey Virginia'daki Amazon Web Services altyapısında, farklı bir bölgede kurulmuş bir DR sitesi ile birden fazla Kullanılabilirlik Bölgesinde barındırılmaktadır. Belirli yedekleme verileri Google Cloud Platform'da (ABD, çoklu bölge) saklanır. Bu veri merkezleri, önde gelen fiziksel ve çevresel güvenlik önlemleri almakta ve bu da son derece esnek bir altyapı sağlamaktadır. Güvenlik uygulamaları hakkında daha fazla bilgiye şu adresten ulaşabilirsiniz:

[AWS güvenlik sayfası](#)

[GCP güvenlik sayfası](#)

21 S: Monday.com hizmeti şirket içi sürümde kullanılabilir mi?

C: Monday.com tamamen bulut tabanlı bir hizmettir ve hizmetinin şirket içi sürümünü sunmaz.

22 S: Veriler ne sıklıkta yedeklenir?

C: Kullanıcı verilerini her 5 dakikada bir yedekler ve şifrelenmiş yedeklemeleri, 25 gün boyunca saklandıkları birden fazla AWS Kullanılabilirlik Alanına dağıtırız. Ayrıca ayrı bir AWS bölgesinde bir olağanüstü durum kurtarma sitesi kurduk. Etkinlik Günlüğü verileri 7 gün boyunca depolandığı GCP'ye (ABD, birden fazla bölge) kadar yedeklenir.

23 S: Monday.com'da Olağanüstü Durum Kurtarma Planı var mı?

C: Evet. DRP'miz, üretim ortamımızı etkileyen felaketlerle ilgilenir ve hizmetin temel işlevlerinin adanmış DR konumumuzdan restorasyonunu içerir. Test yılda en az iki kez yapılır.

24 S: Monday.com'un fiziksel güvenlik politikası var mı?

C: Evet. Hizmetimizin tamamen bulut tabanlıdır ve altyapımızın hiçbir parçası şirket içinde tutulmaz. Ofisimizde fiziksel güvenlik, kişisel tanımlamaya dayalı erişim kontrolü, 7/24 CCTV izleme ve alarm sistemlerini içerir.

25 S: Hizmetinizin kullanılabilirliğini nasıl sağlarsınız?

C: Bir veya daha fazla bileşenin arızalanması durumunda sistem sağlığı üzerinde minimum etkiyi sağlamak için bir mikro hizmet mimarisi kullanıyoruz. Çoklu Kullanılabilirlik Bölgeleri daha fazla çeşitlilik sağlamak için kullanılır ve bazı hizmetler için de güvendiğimiz alternatif sağlayıcılarımız vardır. Kurumsal müşterilere SLA şartlarına tabi olarak %99,9 [SLA](#) sağlanır. Ayrıca, hizmetimizin kullanılabilirliği [durum sayfamızdan](#) izlenebilir ve e-posta veya kısa mesaj yoluyla güncellemeleri almak için abone olunabilir.

26 S: Monday.com güvenli mimari tasarımı için en iyi uygulamaları kullanıyor mu?

C: Evet, kullanıyoruz. AWS Gelişmiş Teknoloji Ortağımız . [AWS Gelişmiş Teknoloji Ortağımız](#). Bu, AWS'nin kendisinin altyapı, güvenlik, en iyi uygulama tasarımı ve daha fazlası açısından monday.com'u titizlikle incelediğine dair bir onay görevi görür.

27 S: Monday.com müşteri verilerinin güvenli bir şekilde silinmesini destekliyor mu?

A: Evet. Hizmetimiz, GCP'ye kadar yedeklenmiş belirli veriler ile AWS üzerinde barındırılmaktadır. Her iki bulut bilgi işlem sağlayıcısı, çok kişili bir ortamda hassas verilerin güvenli bir şekilde depolanmasına ve silinmesine olanak sağlamak için tescilli veri dağıtımı ve silme stratejileri uygular. Depolama ortamının devreden çıkarılması, yukarıda belirtilen sağlayıcılar tarafından NIST 800-88'de açıklanan teknikler kullanılarak gerçekleştirilir.

Olağanüstü durum hazırlığı

28 S: Monday.com'un bir olağanüstü durum yanıt planı var mı?

C: Evet. Olay Yanıt Planımız, olayların tespit edilmesi, ilgili personele iletilmesi, iletişim (iç ve dış), soruşturma, etki azaltma ve olay sonrası analiz için iç yönergeler ortaya koymaktadır.

Daha fazla bilgi [DPAŞ](#)'mızda Bölüm 7 (Veri Olayı Yönetimi ve Bildirimi) bölümünde bulunabilir .

29 S: Bir olay veya ihlalin kişisel verilerimi tehlikeye atması durumunda, monday.com beni nasıl bilgilendirecektir?

C: Olayın şekline, türüne, kapsamına ve ölçeğine bağlı olacaktır, ancak en azından hesap yöneticilerinize gönderilen bir e-posta içerecektir. İhlalin doğası, monday.com'un tespit ettiği zararlı etkileri ve Monday'in yaptığı veya yapmayı planladığı eylemler mümkün olduğunca size bildirilecektir.

Entegrasyon seçenekleri

30 S: monday.com API erişimi sunuyor mu?

C: Evet, GraphQL API'mizdeki belgeleri [burada](#) bulabilirsiniz.

31 S: Monday.com hizmeti ile daha fazla entegrasyonu destekliyor mu?

C: Evet. API'mıza ek olarak, Zoom, Slack, Zendesk, Microsoft Teams, Salesforce, Outlook ve daha fazlası dahil olmak üzere özelleştirilmiş iş akışları oluşturmak için entegrasyonları ve [diğer yazılım çözümlerini](#) destekliyoruz. Bu, yönetici paneli aracılığıyla devre dışı bırakılabilen isteğe bağlı bir özelliktir.