



Autodesk® Fusion 360

Güvenlik Teknik İncelemesi

Ekim 2022



İçindekiler

1. GİRİŞ.....	2
1.1 BELGENİN AMACI VE KAPSAMI	2
2. AUTODESK GÜVENLİĞİ	2
3. FUSİON 360 MÜHENDİSLİK.....	3
3.1 ÇALIŞAN EĞİTİMİ	4
4. FUSİON 360 ÜRÜN GÜVENLİĞİ	4
4.1 İLETİŞİM GÜVENLİĞİ	4
4.2 ŞİFRELEME VE ŞİFRELER	4
4.3 KİMLİK DOĞRULAMA	4
4.4 VERİ GÜVENLİĞİ	5
4.5 TASARIM SÜRÜMÜ	5
4.6 HUB VE GRUP TABANLI İŞ BİRLİĞİ GÜVENLİĞİ.....	5
4.7 ORTAK PAYLAŞIM	5
5. BULUT ALTYAPISI	6
5.1 YÜKSEK KULLANILABİLİRLİK.....	6
5.2 VERİ ÇOĞALTMA VE YEDEKLİLİK	6
5.3 GÜÇ SİSTEMİ YEDEKLİLİĞİ.....	6
5.4 İNTERNET BAĞLANTISI YEDEKLİLİĞİ	6
5.5 FİZİKSEL ALTYAPI GÜVENLİĞİ	6
5.6 TESİS ERİŞİM KONTROLÜ	7
5.7 YANGIN ÖNLEME	7
5.8 İKLİM KONTROLLERİ	7
6. OPERASYONLAR OLAY YÖNETİMİ	7
7. YAMA YÖNETİMİ	8
8. DEĞİŞİKLİK YÖNETİMİ	8
9. KAPASİTE YÖNETİMİ.....	9
10. UYARILAR VE İZLEME.....	9
11. DAĞITIMLAR SIRASINDA SIFIR KESİNTİ SÜRESİ.....	10
12. AUTODESK FUSİON 360 OPERASYONEL KONTROLLER	10
13. AUTODESK GÜVENLİĞİ	11
13.1 GÜVENLİK AÇIĞI TARAMALARI VE SIZMA TESTİ	11
13.2 AĞ GÜVENLİĞİ.....	11
13.3 ŞİFRELEME.....	12
13.4 GİZLİLİK	12
14. KAYNAKLAR.....	12

1. Giriş

Autodesk® Fusion 360™, alanındaki ilk 3B CAD, CAM ve CAE aracıdır. Ürün geliştirme sürecinizi hem Mac hem de PC'de çalışan tek bir bulut tabanlı platforma bağlar. Fusion 360 araçları, web tarayıcılarını ve mobil cihazları da kapsayacak şekilde genişletilen güvenli ve entegre bir konseptten üretime araç seti ile tasarım fikirlerinin hızlı ve kolay bir şekilde keşfedilmesini sağlar.

1.1 Belgenin Amacı ve Kapsamı

Bu belgenin amacı; Autodesk operasyonlarını, yazılım geliştirme sürecini ve ortamda uygulanan güvenlik önlemlerini açıklamaktır. Bu belgede Autodesk Fusion 360, hem Fusion 360 istemci yazılımını hem de Fusion 360 tarayıcı erişim yazılımını ifade eder.

Autodesk'in güvenlik çerçevesi, müşteri bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için endüstri standartlarına dayanmaktadır.

Yüksek kullanılabilirlik ve ölçeklenebilirlik için tasarlanan Fusion 360, müşterilerimize hızlı ve esnek bir bulut hizmeti sunar. Autodesk'in bulut barındırma sağlayıcısı, bulut altyapısında lider olan Amazon Web Services'tır (AWS). Autodesk, AWS bulut hizmetlerini çalıştıran donanım, yazılım, ağ iletişimi ve tesislerden oluşan altyapıyı içeren AWS barındırma sağlayıcısı paylaşılan sorumluluk modeline dayanır. (Daha fazla bilgi için bkz.

<https://aws.amazon.com/tr/compliance/shared-responsibility-model/>).

2. Autodesk Güvenliği

Autodesk güvenlik çerçevesi, tutarlı güvenlik uygulamaları sağlamak için endüstri standartlarını temel alarak güvenli şekilde üretim yapmamızı, çalışmamızı ve güvende kalmamızı sağlar.

- **Güvenli oluşturun** - Ürünlerimize sıfırdan güvenlik eklemek, müşterilerimizin Autodesk ürün ve hizmetlerine yaptığı yatırımı güvence altına almanın kritik bir parçasıdır. Güvenliği yazılım geliştirmenin tüm aşamalarına entegre ediyoruz.
- **Güvenli çalışın** – Güvenliği doğrudan altyapımıza yerleştiririz. Bütünsel yaklaşımımız, uç nokta koruma araçlarının dağıtımını, standartlaştırılmış yama uygulama ve

sağlamlaştırma gereksinimlerini, kimlik ve erişim yönetimi denetimlerini ve saldırgan güvenlik etkinliklerini içerir.

- **Güvende kalın** – Autodesk'te güvenlik; bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini (CIA) koruyan üç temel hedefe odaklanır:
 - Gizlilik: Bilgilere yalnızca yetkili kişiler erişebilir
 - Bütünlük: Bilgi eksiksiz ve doğrudur
 - Kullanılabilirlik: Veriler erişilebilir ve müşteriler tarafından kullanılabilir

Güvenlik Direktörü (CSO), güvenlik stratejisinin ve programının geliştirilmesi, uygulanması ve yönetilmesinden sorumludur ve güvenlik politikalarının ve standartlarının tüm Autodesk ürünlerine ve ortamlarına uygulanmasını sağlar. CSO ve güvenlik ekibi, Autodesk yöneticileri ve Yönetim Kurulu tarafından desteklenmektedir.

3. Fusion 360 Mühendislik

Fusion 360 Mühendislik ekibi, Fusion 360 istemci yazılımını ve bulut hizmetleri uygulamasını tasarlamaktan, uygulamaktan ve test etmekten sorumludur.

Fusion 360'ın tasarımı, kodlanması, test edilmesi ve bakımı, çevik bir yazılım geliştirme sürecine dayanmaktadır. Tasarım sprint'leri sırasında, tasarımın işlevselliğini ve ölçeklenebilirliğini değerlendirmek için mimarlar tarafından ayrıntılı tasarım belgeleri üretilir ve gözden geçirilir. Uygulama sprint'leri sırasında, yazılım mühendisleri ve mimarlar Fusion 360 uygulama geliştirme uygulamalarından sapmaları tespit etmek için eş kod incelemeleri yapar. İşlem sırasında üretilen tüm kodlar işlevsel birim testini içerir ve kalite güvence personeli Tamamlanma Tanımı kriterlerinin kabulünü doğrulayana kadar hiçbir kullanıcı hikâyesi tamamlanmaz. Fusion 360'ın performans testi de geliştirme yaşam döngüsüne entegre edilmiştir. Fusion 360 ekibi, performansı olumsuz yönde etkileyen değişiklikleri sürecin mümkün olduğunca erken bir aşamasında belirlemek için geliştirme sprint'leri boyunca yük testleri gerçekleştirir.

3.1 Çalışan Eğitimi

Tüm Autodesk çalışanları, yeni işe alım oryantasyonunun bir parçası olarak bilgi güvenliğinin önemini teyit etmelidir. Çalışanların, şirketin Davranış Kuralları hakkında bir eğitim kursunu okuması, anlaması ve buna katılması gerekmektedir. Kurallar, her çalışanın işlerini yasal, etik, dürüstlük ve birbirlerine ve şirketin kullanıcılarına, ortaklarına ve rakiplerine saygı duyarak yürütmesini gerektirir.

Autodesk çalışanlarının gizlilik, iş etiği, uygun kullanım ve profesyonel standartlarla ilgili şirket yönergelerine uymaları gerekmektedir. Yeni çalışanlar bir gizlilik sözleşmesi imzalamalıdır. Yeni çalışan oryantasyonu, müşteri verilerinin gizliliğini ve mahremiyetini vurgulamaktadır.

Autodesk, en iyi güvenlik uygulamalarını uygulamak amacıyla Mühendislik ve Bulut Altyapısı işlevlerindeki herkes için yıllık Yazılım Güvenliği Sertifika Programı'nı (SSCP) kullanıma sunmuştur.

4. Fusion 360 Ürün Güvenliği

Autodesk Fusion 360, bulut hizmetleriyle iletişimden kullanıcıların kontrol edebileceği ürün düzeyinde güvenlik ve iş birliği özelliklerine kadar uzanan yerleşik güvenlik özelliklerine sahiptir.

4.1 İletişim Güvenliği

Autodesk Fusion 360 ile bulut hizmetleri arasındaki tüm iletişim, güvenli HTTPS bağlantıları gerektirir.

4.2 Şifreleme ve Şifreler

Fusion 360 ile arka uç hizmetleri arasındaki ve arka uç hizmetleri içindeki iletişim şifreli bir kanal üzerindedir.

4.3 Kimlik Doğrulama

Autodesk Fusion 360'a erişmek için Autodesk kimliği, kullanıcı kimliği ve paroladan oluşan kimlik bilgileri gereklidir. Kimlik bilgileri ağ iletimi sırasında güvence altına alınır ve yalnızca tuzlanmış (salting) hash olarak depolanır.

Fusion 360, son kullanıcılara oturum açarken çok faktörlü kimlik doğrulaması kullanma seçeneği sunar. Bu özelliği etkinleştirmeyi tercih eden kullanıcılar, şifreleriyle birlikte kullanmak üzere bir kod almak için yetkili güvenli kişisel cihazlarını (ör. cep telefonu) kullanabilirler.

4.4 Veri Güvenliği

Tüm Fusion 360 tasarımları bulutta şifreli depolamaya kaydedilir. Depolama çözümü, verileri şifrelemek için 256 bit Gelişmiş Şifreleme Standardı (AES-256) kullanır.

Yerel olarak, önbelleğe alınan tasarımlar erişim denetimi için İşletim Sistemi kullanıcı düzeyi izinlerine dayanır.

4.5 Tasarım Sürümü

Autodesk Fusion 360, her tasarım için bir sürüm geçmişi tutar. Sürüm oluşturma, kullanıcıların önceki sürümlere geri dönmelerine izin vererek ve her dosya değişikliği hakkında bilgi içeren denetlenebilir bir liste sağlayarak verilerin bütünlüğünü korur.

4.6 Hub ve Grup Tabanlı İş Birliği Güvenliği

Projeler, bir dizi ortak çalışan için Autodesk Fusion 360 tasarımlarına erişim izni vermek veya erişimi sınırlamak için basit bir temel sağlar. Proje davetleri, projenin sahibi veya moderatörü tarafından onaylanır ve yeni kullanıcılara erişim izni veren üyeler üzerinde sıkı kontrol sağlar.

Şirketler, üyeler tarafından oluşturulan tüm projelere sahiplik ve erişim denetimi uygulamalarına olanak tanıyan Ekip Hub'larını seçebilir. Açık, kapalı ve gizli projeler gibi proje gizlilik ayarları, kontrollü iş birliğine olanak tanır. Ekip Hub'ları ile, üyeler projeye davet edilen ortak çalışanlara erişimi kısıtlamayı seçebilir. Ekip Hub'ları ayrıca müşteri yöneticilerinin eski çalışanların hesaplarını devre dışı bırakmasına ve proje sahipliğini ekipteki diğer üyelere aktarmasına olanak tanır.

4.7 Ortak Paylaşım

Ortak Paylaşım ile kullanıcılar, Autodesk kimliği veya Fusion 360 yetkilendirmesine sahip olmayan dış paydaşlarla iş birliği yapabilir. Fusion 360 kullanıcıları, tasarıma salt okunur erişim sağlayan bir bağlantı oluşturur. Kullanıcılar ayrıca indirme/dışa aktarma özelliklerini etkinleştirme seçeneğine de sahiptir. Kullanıcı, istediği zaman bu bağlantı tarafından sunulan herkese ortak paylaşımı iptal edebilir.

5. Bulut Altyapısı

Bulut Altyapısı ekibi, uygulama sürümü yönetimi, donanım ve işletim sistemi yükseltmeleri, sistem durumunu izleme ve Autodesk Fusion 360'ı sürdürmek için gereken diğer etkinliklere yönelik prosedürleri tanımlamaktan ve yürütmekten sorumludur.

5.1 Yüksek Kullanılabilirlik

Autodesk Fusion 360, destekleyici altyapısında yedekli sistemler kullanarak ve yükü ölçeklenebilir bir bulut sunucusu filosuna dağıtarak yüksek düzeyde erişilebilirlik elde etmek üzere tasarlanmıştır.

5.2 Veri Çoğaltma ve Yedeklilik

Müşteri verileri çoğaltması, Amazon Web Services (AWS) Erişilebilirlik Alanları (AZ'ler) arasında gerçekleştirilir. Çoğaltma, bir yedek veri merkezine yük devretme gerekiyorsa veri kaybı veya hizmetin yeniden başlatılmasında gecikme olasılığını sınırlar.

5.3 Güç Sistemi Yedekliliği

AWS veri merkezleri, operasyonları haftanın yedi günü, günün 24 saati sürdürmek için yedekli elektrik güç sistemleri içerir. Kesintisiz Güç Kaynakları (UPS'ler), bir arıza durumunda birincil elektrik sistemlerine otomatik olarak yedekleme sağlar. Her veri merkezindeki jeneratörler, bir kesinti meydana gelirse uzun süreli yedek güç sağlar.

5.4 İnternet Bağlantısı Yedekliliği

Veri merkezlerinin her birine İnternet bağlantısını sürdürmek için yedekli bir çok satıcılı sistem kullanılır.

Autodesk Fusion 360 istemci yazılımı, kullanıcıların internete bağlı olmadıklarında tasarımlarının yerel kopyalarına erişmeye ve bunlar üzerinde çalışmaya devam etmelerini sağlayan çevrimdışı bir moda da sahiptir.

5.5 Fiziksel Altyapı Güvenliği

Autodesk Fusion 360 uygulaması, çeşitli güvenlik denetimleriyle yetkisiz fiziksel erişime ve çevresel tehlikelere karşı korunan AWS güvenli veri merkezlerinde çalışır. Bazı fiziksel ve çevresel kontroller aşağıda özetlenmiştir. AWS Güvenlik Süreçlerine tam bir genel bakışa [buradan](#) ulaşabilirsiniz.

5.6 Tesis Erişim Kontrolü

AWS veri merkezleri, profesyonel fiziksel güvenlik personeli tarafından haftanın 7 günü, günün 24 saati korunur. Her veri merkezinin çevresinin yanı sıra bilgi işlem ve destek ekipmanı içeren odalar video gözetimi ile korunmaktadır. Video gözetimi, son etkinliklerin talep üzerine görüntülenmesini sağlayan dijital medyada korunur. Veri merkezi girişleri, aynı anda tek bir kişiye erişimi kısıtlayan tuzaklar tarafından korunmaktadır. Tüm ziyaretçiler ve yükleniciler, kabul edilmek için kimlik ibraz etmeli ve her zaman yetkili personel tarafından eşlik edilmelidir. Yalnızca meşru bir iş ihtiyacı olan çalışanlara veri merkezi erişimi sağlanır ve tüm ziyaretler elektronik olarak günlüğe kaydedilir.

5.7 Yangın Önleme

Duman alarmları ve ısıt aktivasyonlu ıslak borular gibi yangın algılama ve söndürme sistemleri, bilgi işlem ekipmanı ve destek sistemleri içeren odaları korumak için her veri merkezine kurulur. Yangın algılama sensörleri tavana ve yükseltilmiş zeminin altına monte edilmiştir.

5.8 İklim Kontrolleri

Veri merkezi iklim kontrolleri, katı çevresel aralıkların ihlal edilmesi durumunda sunucuları, yönlendiricileri ve arızaya maruz kalan diğer ekipmanları korur. Aşırı ısınma gibi tehlikeli koşulların oluşmasını önlemek için hem sistemler hem de personel tarafından izleme yapılmaktadır. Sıcaklık ve diğer çevresel ölçümleri kabul edilebilir aralıklarda tutan ayarlamalar, kontrol sistemleri tarafından otomatik olarak yapılır.

6. Operasyonlar Olay Yönetimi

Autodesk, olay çözümülemesini teşvik etmek için en iyi uygulamaları tanımlayan bir olay yönetimi ilkesine sahiptir. Autodesk olay yönetimi ilkesi, düzeltilebilir yordamlardan oluşan bir bilgi tabanı oluşturmak için düzeltme adımlarının günlüğe kaydedilmesini ve kök neden analizinin kullanılmasını vurgular. Autodesk olay yönetimi ilkesinin amacı yalnızca olayları hızlı ve etkili bir şekilde kapatmak değil, aynı zamanda süreçlerin sürekli iyileştirilmesi ve gelecekteki yanıtların birikmiş bilgi birikimi tarafından yönlendirilmesi için olay bilgilerini toplamak ve dağıtmaktır.

7. Yama Yönetimi

Bulut Altyapısı ekibi, etkili yama dağıtımı sağlamaya yardımcı olan bir yama yönetimi ilkesine sahiptir. Mümkün olduğunda, yeni yamaları kontrol etmek ve yetkili Bulut Altyapısı personeli tarafından onaylanabilecek dağıtım listeleri hazırlamak için otomasyon uygulanır. Yama uygulama ilkesi, bir yamanın sistem kararlılığı üzerindeki etkisini belirlemeye yönelik ölçütleri de tanımlar. Bir yamanın muhtemelen yüksek bir etkiye sahip olduğu belirlenirse, yama dağıtılmadan önce regresyon testi tamamlanır. Değişiklik Yönetimi, yamaların üretim sistemlerine dağıtımını izler.

8. Değişiklik Yönetimi

Bulut Altyapısı ekibi, aşağıdaki etkinlikleri içeren bir değişiklik yönetimi ilkesine sahiptir:

- **Değişiklik Talebi (RFC) formu.** Tüm değişiklikler için bir RFC formu gönderilmelidir. Form, değişikliği başlatanın adını, değişiklik önceliğini, değişikliğin iş gerekçesini ve talep edilen değişikliğin uygulama tarihini içerir.
- **Geri alma planları.** Bulut Altyapısı ekibi, bir değişikliğin hizmet kesintisine neden olması durumunda sistem durumunun geri yüklenebilmesi için dağıtımdan önce ayrıntılı geri alma planları oluşturur. Geri alma planları, sistem durumunu en az manuel adımla geri yükleyen komut dosyalarında tanımlanan yürütülebilir talimatları içerir.
- **Tanımlı bakım dönemleri.** Bulut Altyapısı ekibi zamanlanmış, acil durum ve genişletilmiş bakım dönemlerini belirtir. Yoğun olmayan saatlerde planlı bakım planlarlar.
- **Test planı.** Bulut Altyapısı ekibi, bir değişikliğin dağıtımdan sonra işlevselliğin erişilebilir olduğunu doğrulamak için bir dizi test tanımlar.
- **Test yürütme.** Dağıtım tamamlandıktan sonra, Bulut Altyapısı ve Autodesk Fusion 360 Kalite Güvencesi ekibi, risk altında olarak tanımlanan işlevlerin kullanılabilir durumda olup olmadığını kontrol etmek için testleri yürütür.

9. Kapasite Yönetimi

Bulut hizmetlerine müşteri erişimi self servis modeli aracılığıyla isteğe bağlı olarak sağlandığından, trafik desenleri oldukça değişkendir ve ani kullanım artışlarına tabidir. Bir ani artış meydana geldiğinde, hizmeti destekleyen bilgi işlem kaynakları havuzu tükenirse hizmetin kullanılabilirliği olumsuz etkilenebilir. Bulut Altyapısı ekibi, yüksek düzeyde kullanılabilirlik sağlamak için bir kapasite yönetimi ilkesi uygular. Bu uygulamalar şunları içerir:

- **Kaynak kullanımının sıkça kaydedilmesi.** Autodesk Fusion 360 kaynak kullanımı; sanal örnekler, sanal depolama birimleri ve sanal ağ cihazları dahil olmak üzere çeşitli altyapı bileşenlerinde sık aralıklarla toplanır. Kullanım istatistikleri bir kapasite yönetimi deposunda depolanır.
- **Kapasite planlama.** Bulut Altyapısı ekibi, mevcut kullanım düzeylerini belgeleyen ve istatistiksel analize ve yaklaşan geliştirmelerin iş işlevselliğine yönelik etkisine dayalı olarak gelecekteki düzeyleri modelleyen ayrıntılı bir kapasite planı oluşturmak için kapasite yönetimini kullanır. Kapasite planı, gerektiğinde veya kullanım modellerinde önemli değişiklikler algılandığında güncellenir.
- **Kaynak tahsisi.** Hesaplama kaynakları, müşterilerin talep ettiği şekilde tahsis edilir. Önceden ısıtılmış hesaplama kaynakları her zaman kullanılabilir. Bir etkinlik artışı olursa, yeni kaynakların örneği oluşturulur. Örneğin, Autodesk Fusion tarayıcı kaynaklarının kullanılabilirliği genellikle 10 dakikadan kısa sürede elde edilir.
- **Etkinlik izleme.** Etkinlik panoları ve uyarıları, arka uç hizmetleri genelinde tanımlanarak mühendislerin sistem etkinliğini gözlemlemesine ve olay sonrası incelemeler ve analizler yapmasına olanak tanır.

10. Uyarılar ve İzleme

Autodesk, mümkün olan en kısa Ortalama Düzeltme Süresini sağlamak amacıyla Fusion 360'ı izlemek için otomatik sistemler kullanır ve hizmetin sistem durumunu doğrular. Veritabanından hizmetlere kadar her bir bileşen ayrı ayrı izlenir.

Hizmeti etkileyen bir olay olması durumunda, uyarılar oluşturulur ve Bulut Altyapısı ekibi bir yükseltme işlemi aracılığıyla bilgilendirilir.

Hizmet durumu, Autodesk hizmetleri arasındaki karşılıklı ilişkiyi de açıklar. Autodesk Fusion 360 gibi bir hizmet, ACM hizmetine (Erişim Kontrolü) karşı son derece hassastır. Bağlı bir hizmet başarısız olduğunda her hizmetin dayanıklı olması ve müşteri için herhangi bir veri kaybı olmadan artık çalışmadığında düzgün bir şekilde başarısız olması gerekir.

Fusion 360 hizmetinin durumu, Autodesk'in Sağlık Panosu Hizmeti tarafından herkese açık olarak görüntülenir: <https://health.autodesk.com>.

11. Dağıtımlar Sırasında Sıfır Kesinti Süresi

Yamalar üretim ortamına uygulandıkça, Autodesk Fusion tarayıcısı ve diğer Fusion 360 hizmetleri için [Mavi-Yeşil dağıtım](#) yaklaşımı benimsenir. Bu, müşterilerin hizmette herhangi bir kesinti yaşamamasını sağlamaya yardımcı olur.

12. Autodesk Fusion 360 Operasyonel Kontroller

Autodesk Fusion 360, hassas müşteri verilerinin yetkisiz erişime karşı korunmasını sağlar.

- **Veri merkezlerine yönelik fiziksel kısıtlamalar.** Veri merkezlerine yönelik fiziksel kısıtlamalar, yetkisiz tarafların Autodesk Fusion 360 tarafından kullanılan donanım ve destek sistemlerine erişmesini engeller.
- **Arka plan kontrolleri.** Autodesk Fusion 360 tarafından kullanılan bilgi işlem kaynaklarına ve destek sistemlerine fiziksel erişimi olan çalışanlar için geçmiş kontrolleri gereklidir.
- **Veri çoğaltma.** Veri çoğaltma, müşteri verilerini yedekli veri merkezlerine kopyalar, böylece tesisler arasında yük devretme gerçekleşirse iş sürekliliği korunabilir.
- **Yedekli teknolojiler.** Yük dengeleyiciler ve kümelenmiş veritabanları gibi yedekli teknolojiler, tek hata noktalarını sınırlar.

13. Autodesk Güvenliği

Autodesk Güvenliği ekibi, Autodesk bulut ortamındaki güvenlik uygulamalarını tanımlamaya ve uygulamaya odaklanmış özel bir bilgi güvenliği uzmanları grubudur. Autodesk Güvenliği ekibinin sorumlulukları şunlardır:

- Autodesk'in bulut altyapısı tasarım ve uygulamasının güvenlik duruşunu gözden geçirme.
- Kimlik ve erişim yönetimi, parola yönetimi ve güvenlik açığı yönetimi dahil olmak üzere güvenlik ilkelerinin tanımlanması ve uygulanmasının sağlanması.
- Dahili incelemeler ve denetimler yaparak yerleşik güvenlik prosedürlerine uyumu sağlama.
- Müşteri bilgilerini güvence altına alan teknolojilerin belirlenmesi ve uygulanması
- Bilgi güvenliği değerlendirmeleri yapmak için üçüncü taraf güvenlik uzmanlarını görevlendirme
- Bulut hizmetlerini olası güvenlik sorunları için izleme ve olaylara gerektiği gibi yanıt verme
- Autodesk'in güvenlik politikasının yıllık incelemelerini yapma.

13.1 Güvenlik Açığı Taramaları ve Sızma Testi

Fusion 360 hizmetleri, yıllık sızma testine tabi tutulur ve güvenlik tehditleri ve güvenlik açıkları için düzenli taramalardan geçer. Uygulama ayrıca statik analize ve üçüncü taraf kütüphane taramalarına tabi tutulur. Güvenlik taramaları ve sızma testleri, Open Web Application Security Project (OWASP) ve SANS top 25 tarafından tanımlanan çok çeşitli güvenlik açıklarını kapsar.

13.2 Ağ Güvenliği

Ağ güvenliği, şifreleme, güvenlik duvarları ve sistem sağlamlaştırma yordamları dahil olmak üzere fiziksel ve mantıksal denetimlerin bir birleşimi kullanılarak uygulanır. Ayrıca AWS, fiziksel veri merkezlerini koruyan ağ güvenliği denetimleri sağlar. Daha fazla bilgi için bkz: [Güvenlik, Kimlik ve Uyumluluk İçin En İyi Uygulamalar](#).

13.3 Şifreleme

Tüm ağ trafiği, İnternet üzerinden Autodesk bulut ortamının çevresine iletildiğinde şifrelenir. Kimlik bilgileri, uygulama oturumu bilgileri, erişim belirteçleri ve kullanıcı profilleri gibi hassas bilgiler bekleme durumundayken şifrelenir.

13.4 Gizlilik

Autodesk, müşterilerin kişisel verilerinin nasıl toplandığı ve kullanıldığı konusunda şeffaftır. Daha fazla bilgi edinmek için Autodesk [Gizlilik Bildirimi](#)'ni okuyun.

14. Kaynaklar

Aşağıdaki kaynaklar, Autodesk ve bu belgenin ana bölümünde başvurulanan diğer konular hakkında genel bilgiler sağlar.

- **Autodesk** – Autodesk hakkındaki bilgileri görüntülemek için <https://www.autodesk.com.tr> adresini ziyaret edin.
- **Autodesk Güven Merkezi** – Autodesk Güven Merkezi hakkındaki bilgileri görüntülemek için <http://trust.autodesk.com> adresini ziyaret edin.
- **Autodesk Fusion 360** – Fusion 360 hakkındaki bilgileri görüntülemek için <http://fusion360.autodesk.com> adresini ziyaret edin.

Bu belgede yer alan bilgiler, Autodesk, Inc.'in yayın tarihi itibarıyla geçerli görünümünü temsil eder ve Autodesk bu bilgilerin güncellenmesi konusunda hiçbir sorumluluk kabul etmez. Autodesk, ürün veya hizmetlerinde zaman zaman iyileştirmeler ve başka değişiklikler yapar, bu nedenle içindeki bilgiler yalnızca yayınlanma tarihi itibarıyla sunulan Autodesk Fusion 360 sürümü için geçerlidir. Bu teknik inceleme yalnızca bilgilendirme amaçlıdır. Autodesk, bu belgede açık veya zımni hiçbir garanti vermez ve bu teknik incelemedeki bilgiler, Autodesk adına bağlayıcı bir yükümlülük veya taahhüt oluşturmaz. Yukarıda belirtilenleri sınırlandırmadan veya değiştirmeden, Autodesk Fusion 360 hizmetleri, <http://www.autodesk.com/company/legal-notices-trademarks/terms-of-service-autodesk360-web-services> adresinde bulunan geçerli hizmet koşullarına tabi olarak sağlanır. Autodesk, Autodesk Logosu ve Fusion 360 Autodesk, Inc. şirketine ve/veya ABD'de ve/veya diğer ülkelerdeki bağlı kuruluşlarına ve/veya iştiraklerine ait ticari markalar ya da tescilli ticari markalardır. Diğer marka adları, ürün adları veya ticari markalar, sahiplerine aittir. Autodesk, haber vermeksizin herhangi bir zamanda ürün ve hizmet tekliflerini ve özelliklerini değiştirme hakkını saklı tutar ve bu belgede ortaya çıkabilecek baskı veya grafik hatalarından sorumlu değildir. © 2022 Autodesk, Inc. Tüm hakları saklıdır.