



## Google Apps ile ilgili güvenlik açığı korumaları ve kapsamlı güvenlik incelemesi

Google teknik makalesi, Şubat 2007

# Google Apps'in güvenliđi



---

## DAHA FAZLA BİLGİ İÇİN

---

**Online** [www.google.com/a](http://www.google.com/a)

**E-posta** [apps-enterprise@google.com](mailto:apps-enterprise@google.com)

---

Herhangi bir sistemde başarıyı garanti etmenin anahtarı, sözde bilgisayar korsanlarına karşı ağ tabanlı uygulamaların güvenliğini sağlamaktır. E-posta ve ortak çalışma söz konusu olduğunda güvenlik son derece önemlidir. Google, Google Apps'teki verilerin güvenli, emin ve gizli kalması için teknolojiye, insanlara ve süreçlere milyarlarca dolar yatırım yapmaktadır. Google'ın güvenlik uzmanlarından oluşan özel ekibi, Google'ın sıkı güvenlik ve veri gizliliđi standartlarını tutturmak için, daha en başından güvenlik özelliklerini tasarlama ve tüm tasarım, kod ve son ürün süreçlerini gözden geçirme sorumluluđu taşır. Google Apps'i barındırmak ve yüz binlerce kullanıcı verisini güvende tutmak için kullanılan altyapının aynısı, reklamcılık işlemlerinde milyarlarca doları ve milyonlarca tüketici verisini yönetmek için de kullanılır. Google Apps ile bilgiler güvende ve sağlamdır.

GİRİŞ	3
ÖRGÜTSEL GÜVENLİK VE İŞLEM GÜVENLİĐİ	3
Geliştirme Metodolojisi	4
İşlem Güvenliđi	4
Güvenlik Topluluđu ve Danışmanlar	4
VERİ GÜVENLİĐİ	4
Fiziksel Güvenlik	4
Mantıksal Güvenlik	5
Bilgilerin Erişilebilirliđi	5
Yedek Kapasite	6
TEHDİTLERDEN KAÇINMA	6
Spam ve Virüs Koruması	6
Uygulama ve Ağ Saldırıları	6
GÜVENLİ ERİŞİM	7
Son kullanıcıyı koruma özellikleri	7
Denetim Sizde	7
VERİ GİZLİLİĐİ	8
SONUÇ	8



## **Giriş**

Google, dünya genelinde bilgileri düzenleme misyonunun bir parçası olarak on milyonlarca kullanıcıya ait verilerin güvenliğini sağlamaktan sorumludur. Google bu sorumluluğu çok ciddiye alır; kullanıcılarının güvenliğini kazanmak ve bu güvene layık olma yolunda büyük çaba harcamaktadır. Google, güvenli ürünlerin kullanıcının duyduğu güveni korumaya yardımcı olduğunu bilir ve kullanıcıların gereksinimlerini karşılayıp, tümüyle onların çıkarına hizmet eden yenilikçi ürünler oluşturmaya gayret eder.

Google Apps, güvenli ve güvenilir ürünler üretirken bu büyük işlem deneyiminden faydalanır. Google'ın ürün ve hizmetleri, müşteri ve kullanıcı verilerinin güvende olmasını sağlamak için, gelişmiş teknoloji çözümleriyle endüstrinin önde gelen güvenlik uygulamalarını bir araya getirir. Veri ve uygulamalar için en güvenli ve güvenilir ortamı sağlamak amacıyla, milyarlarca dolarlık sermaye yatırımı yapılmaktadır. Google özellikle de, güvenliğin iş müşterileri açısından kritik bazı yönlerine odaklanmaktadır:

- Örgütsel Güvenlik ve İşlem Güvenliği – Tasarım, uygulama ve devam eden işlemlerin her aşamasında güvenliği sağlamaya yönelik ilke ve prosedürler.
- Veri Güvenliği – Müşteri verilerinin güvenli tesislerde, güvenli sunucularda ve güvenli uygulamalar içinde saklanmasının sağlanması.
- Tehditlerden Kaçınma – Kullanıcıların ve kullanıcı bilgilerinin kötü niyetli saldırılara ve sözde bilgisayar korsanlarına karşı korunması.
- Güvenli Erişim – Verilere yalnızca yetkili kullanıcıların erişebilmesinin ve erişim kanalının güvenli olmasının sağlanması.
- Veri Gizliliği – Gizli bilgilerin hususi ve gizli tutulmasının sağlanması.

Bu belgede, en üst düzeyde veri güvenliği ve gizliliğinin temini için birçok fiziksel, mantıksal ve işlemsel güvenlik önleminin kullanıldığı Google güvenlik stratejisi ele alınmaktadır.

## **Örgütsel Güvenlik ve İşlem Güvenliği**

Google'ın güvenlik stratejisinin temeli, Google çalışanları ve süreçlerinden başlar. Güvenlik; uygun şekilde bir araya getirdiğimizde güvenli ve sorumlu bilgi işleme sağlayan kişilerin, süreçlerin ve teknolojilerin bir birleşimidir. Güvenlik, sonuçlara bakarak geçerliliği denetlenebilecek bir unsur değildir. Daha ziyade, ürün, mimari, altyapı ve sistemlerin tasarımına en başından itibaren katılır. Google kapsamlı güvenlik politikaları geliştirmek, bunları belgelemek ve uygulamak için tam gün çalışan bir güvenlik ekibine görev verir. Google'ın Güvenlik ekibi, bilgi, uygulama ve ağ güvenliği konusunda dünyanın önde gelen bazı uzmanlarından oluşur.

Bu güvenlik ekibi çevre savunması, altyapı savunması, uygulama savunması, güvenlik açıklarını algılama ve bunlara karşılık verme gibi işlevsel alanlara ayrılır. Birçoğu, Fortune 500 listesinde yer alan şirketlerde üst düzey bilgi güvenliği rollerinde edindikleri deneyimle Google'a gelmiştir. Bu ekip, çabalarının büyük bir bölümünü kod ve sistemlerin en başından güvenli olmasını sağlamaya yönelik önleyici tedbirler üzerine yoğunlaştırmakta olup, güvenlik sorunlarına dinamik olarak karşılık vermeye her an hazırdır.

### **Geliştirme Metodolojisi**

Google'ın güvenliğe bakışı, bir tasarım ürünü taslak haline getirildiği andan başlayarak her zaman çok önemlidir. Google'ın mühendislik ve ürün ekipleri güvenlik esasları konusunda kapsamlı bir eğitim alır. Google'ın geliştirme metodolojisi, sürekli kontrol noktaları ve eksiksiz denetimleri içeren çok adımlı bir plan ortaya koyar.

Google Uygulama Güvenliği Ekibi, tasarım inceleme, kod denetimi, sistem ve işlevsel testlerin yanı sıra en son piyasaya sürme onayı dahil, ürün geliştirme döngüsünün tüm aşamalarında rol oynar. Google, uygulamaların her düzeyde güvenli olmasını sağlamak için, birçok ticari ve tescilli teknolojiye yararlanır. Google Uygulama Güvenliği ekibi aynı zamanda, müşteri güvenliğinin temini için güvenli geliştirme süreçlerine uyulmasını sağlamaktan sorumludur.

### **İşlem Güvenliği**

Google Güvenlik İşlemleri ekibi, veri işleme ve sistem yönetimi de içinde olmak üzere çalışma sistemlerinin güvenliğini korumaya odaklanır. Bu ekibin üyeleri, veri merkezi işlemlerini rutin olarak denetler ve Google'ın fiziksel ve mantıksal varlıklarına yönelik tehditleri sürekli olarak değerlendirir.

Bu grup aynı zamanda, tüm çalışanların uygun elemelerden geçmesini ve işlerini profesyonel ve güvenli bir biçimde yürütecek eğitimi almalarını sağlamaktan sorumludur. Google, uygun olduğu hallerde, bir çalışanın kuruluşa katılmasından önce geçmişini çok ayrıntılı bir şekilde tarar ve doğrular. Güvenlik süreçlerini ve prosedürlerini korumaktan sorumlu tüm personel uygulamalar konusunda kapsamlı bir eğitim alır ve eğitimleri sürekli güncellenir.

### **Güvenlik Topluluğu ve Danışmanlar**

Google, yukarıda anlatılan süreçlere ek olarak, güvenlik topluluklarıyla etkin bir çalışma içinde bulunarak dünyanın en iyi ve en parlak beyinlerinin ortak görüşlerinden yararlanır. Bu yaklaşım, Google'ın güvenlik trendlerinin gerisinde kalmamasına, ortaya çıkan tehditlere hızla karşılık vermesine ve şirket içindekilerin ve dışındakilerin uzmanlığını bir araya getirmesine yardımcı olur. Google, bu büyük güvenlik topluluğuyla, sorumlu açıklama kapsamında aktif bir etkileşim içindedir. Hem bu program, hem de Google'ın sürekli diyalog içinde bulunduğu bazı önemli güvenlik uzmanları hakkında daha fazla bilgi edinmek için <http://www.google.com/corporate/security.html> sitesini ziyaret edin.

Tüm bu koruma düzeyleri varken bile bilinmeyen güvenlik açıkları ortaya çıkabilir; Google güvenlik uyarıları ve güvenlik açıklarına hızla karşılık verecek donanımına sahiptir. Google Güvenlik ekibi, tüm altyapıyı olası güvenlik açıklarına karşı denetler ve bilinen tüm sorunları hemen gidermek üzere doğrudan mühendislik bölümüyle birlikte çalışır. Kullanıcıyı etkileyen güvenlik sorunları, mümkün olan en kısa sürede e-posta yoluyla Google Apps Kurumsal Sürüm müşterilerine bildirilir.

### **Veri Güvenliği**

Şirket ve kullanıcı verilerinin güvenliği Google'ın Güvenlik ve İşlemler ekibinin misyonudur. Google'ın iş anlayışının kullanıcı güvenine dayanması nedeniyle, kurum olarak Google'ın başarısının sürekliliğinde en önemli unsurlardan biri budur. Son kullanıcıya karşı sorumluluk bilinci tüm Google çalışanlarına telkin edilir. Verilerin korunması tüm Google anlayışının temelini oluşturur. Google milyarlarca dolarlık müşteri ve reklam işlemlerini korumak için olağanüstü bir özen sergiler; aynı özeni Google'ın iletişim ve ortak çalışmaya yönelik teknolojileri için de gösteririz.

Şirket olarak, anlayışımızın temelinde bu düşüncenin yattığını görmek için <http://investor.google.com/conduct.html> sitesinde davranış kurallarımızı inceleyebilirsiniz.

**Fiziksel Güvenlik**

Google, dünyadaki en büyük dağıtımli veri merkezi ağlarından birini işletmekte olup, bu merkezlerde verileri ve fikri mülkiyetleri korumak için büyük çaba harcamaktadır. Google veri merkezlerini dünya genelinde işletmektedir ve birçok Google veri merkezi tamamen kendi sahipliğinde olup, hiçbir dış tarafın erişim sağlayamayacağı şekilde yönetilmektedir. Veri merkezlerinin coğrafi konumları felaket olaylarına karşı koruma sağlayacak şekilde seçilmiştir. Veri merkezi tesislerine ve bu merkezlerde bulunan sunuculara yalnızca belirli Google çalışanlarının erişimi vardır; bu erişim sıkı bir şekilde denetlenmekte ve izlenmektedir. Güvenlik, hem yerel olarak tesislerde, hem de merkezi olarak Google'ın dünya çapındaki güvenlik işlemleri merkezlerinde izlenmekte ve kontrol altında tutulmaktadır.

Tesisler tasarlanırken, yalnızca en üst düzey verimlilik değil, güvenlik ve güvenilirlik de göz önünde bulundurulur. Çoklu düzeyde yedek kapasite olanakları, en zorlu ve korkunç koşullarda bile kesintisiz işlem yapılabilmesini ve hizmet verilebilmesini sağlar. Belirli bir merkez içinde çok düzeyde yedek kapasite, işlemlerin kesintiye uğramaması için jeneratörle çalışan yedek ve birçok dağıtık merkez genelinde tam yedek kapasite olanakları buna dahildir. Merkezleri hem yerel olarak, hem de uzaktan izlemek için ileri teknoloji ürünü kontroller kullanılmaktadır ve sistemleri korumaya yönelik otomatik arızada devir sistemleri mevcuttur.

**Mantıksal Güvenlik**

Web tabanlı bilgi işlemde, verilerin ve uygulamaların mantıksal güvenliği en az fiziksel güvenlik kadar önemlidir. Google, uygulamaların güvenli olmasını, verilerin güvenli ve sorumlu bir yolla işlenmesini, müşteri veya kullanıcı verilerine dışarıdan hiçbir yetkisiz erişimin olmamasını sağlamak için son derece büyük bir çaba göstermektedir. Google, bu amaca ulaşmak için endüstride standart olarak kullanılan bazı tekniklerin yanı sıra bazı benzersiz, yenilikçi yaklaşımlardan da yararlanır. Bu tür yaklaşımlardan biri, genel amaçlı yazılımlara karşılık özel amaçlı teknolojilerden yararlanmaktır.

Google teknolojisinin büyük bir bölümü, genel amaçlı bilgi işleme karşılık özel amaçlı yetenekler sağlamak için yazılır. Örneğin, web sunucusu katmanı, yalnızca belirli uygulamaların çalışması için gerekli özellikleri açığa çıkarmak üzere Google tarafından özel olarak tasarlanıp uygulamaya geçirilir. Bu nedenle, çoğu ticari yazılımın etkilenebileceği çok çeşitli saldırılara karşı bu yazılımlar kadar savunmasız değildir.

Google ayrıca, güvenlik gerekçeleriyle çekirdek kitaplıklarda da değişiklik yapmıştır. Google altyapısı, genel amaçlı bir bilgisayar platformundan çok özel amaçlı bir uygulama sistemi olduğundan, standart Linux işletim sisteminin sağladığı birçok hizmet sınırlandırılabilir veya devre dışı bırakılabilmektedir. Bu değişiklikler, ilgili görev için gerekli sistem özelliklerini artırmaya ve sistemin, zorunlu olmayan ve kötüye kullanılabilir açıklarını devre dışı bırakmaya veya kaldırmaya odaklanır.

Google'ın sunucuları ayrıca, saldırılara karşı savunma için çok düzeyli güvenlik duvarlarıyla korunmaktadır. Trafik saldırı girişimlerine karşı uygun şekilde denetlenir ve kullanıcıların verilerini korumak için her tür saldırı girişimi dikkate alınır.

**Bilgilerin Erişilebilirliği**

E-posta gibi veriler, geleneksel dosya sistemi veya veritabanı biçiminde saklanmak yerine, performans açısından en iyi duruma getirilmiş şifreli biçimde saklanır. Veriler, yedek kapasite amacıyla ve uygunsuz erişim açısından birçok fiziksel ve mantıksal birime dağıtılarak, dışarıdan müdahaleye karşı şaşırtma yapılır. Google'ın yukarıda anlatılan fiziksel koruma özellikleri, sunucuya fiziksel bir erişim sağlanamamasını garanti eder. Üretim sistemlerine tüm erişim, şifreli SSH (güvenli kabuk) kullanan personel tarafından yürütülür. Son kullanıcı verilerine anlamlı erişim için, veri yapılarının ve Google'ın mülkiyetindeki altyapının özel olarak bilinmesi gerekir. Bu özellik, Google Apps içindeki duyarlı verilerin güvenliğini sağlamaya yönelik birçok güvenlik katmanından biridir.





