Apple at Work

Platform Güvenliği

Güvenli tasarım.

Apple'da hem kullanıcıyı hem de kurumsal verileri korumak için güvenliğe büyük önem veriyoruz. Ürünlerimizi en başından itibaren gelişmiş güvenlik özellikleriyle tasarlıyoruz. Bunu mükemmel bir kullanıcı deneyimiyle dengeli olacak şekilde yaparak kullanıcılara istedikleri gibi çalışma özgürlüğünü veriyoruz. Bu kapsamlı bir güvenlik yaklaşımını yalnızca Apple sunabiliyor, çünkü bir ürünlerimizi geliştirirken entegre donanım, yazılım ve hizmetlerden faydalanıyoruz.

Donanım güvenliği
Güvenli yazılımlar için donanımların da temel güvenlik özellikleriyle tasarlanması gerekir. İşte bu nedenle iOS, iPadOS, macOS, tvOS veya watchOS yüklü Apple aygıtları çip üzerinde güvenlik özellikleriyle tasarlanıyor.

Bunlar arasında sistem güvenliği özelliklerine güç veren CPU becerileri ve güvenlik işlevlerine özel ek bir çip yer alıyor. Güvenlik odaklı donanım, saldırı yüzeyini en aza indirmek için sınırlı ve ayrı ayrı tanımlanmış işlevleri destekleme ilkesiyle çalışıyor. Bu bileşenler arasında güvenli başlatma için donanım tabanlı güvenilirlik oluşturan başlatma ROM'u, verimli ve güvenli şifreleme ve şifre çözme için özel AES motorları ve Secure Enclave bulunuyor.

Secure Enclave, tüm yeni nesil iPhone, iPad, Apple Watch, Apple TV ve HomePod aygıtlarının yanı sıra Apple çipe sahip Mac'te ve Apple T2 Security Chip'e sahip Mac'lerde bulunan bir system on a chip (SoC) teknolojisi. SoC teknolojisiyle aynı tasarım prensibine sahip Secure Enclave, ayrık başlatma ROM'unu ve AES motorunu içerir. Secure Enclave, kullanımda olmayan verileri şifrelemek için gereken anahtarların güvenli bir şekilde oluşturulması ve depolanması için de temel sağlar. Ayrıca Touch ID ve Face ID için biyometrik verileri korur ve değerlendirir.

Depolanan verilerin hızlı ve verimli bir şekilde şifrelenmesi gerekir. Aynı zamanda bu işlem sırasında kriptografik anahtarlama ilişkileri için kullanılan verilerin (veya anahtarlama materyallerinin) açığa çıkarılmaması gerekir. AES donanım motoru, bu sorunu dosyalar yazılırken veya okunurken hızlı satır içi şifreleme ve şifre çözmeyle halleder. Secure Enclave'ın özel bir kanalı, gerekli anahtarlama materyallerini uygulama işlemcisine (veya CPU'ya) ya da genel işletim sistemine göstermeden

AES motoruna iletir. Bu sayede Apple Veri Koruma ve FileVault teknolojileri uzun ömürlü şifreleme anahtarlarını açığa çıkarmadan kullanıcı dosyalarını koruyabiliyor.

Apple, en alt yazılım seviyelerini dışarıdan müdahaleye karşı korumak ve sistem başlatılırken yalnızca Apple'ın güvenilen işletim sistemi yazılımlarının yüklenmesine izin vermek için güvenli başlatma özelliğini tasarladı. Güvenli başlatma, Boot ROM adı verilen ve Apple SoC biriminin üretimi sırasında entegre edilen değişmez bir kodda başlar ve donanım güvenliğinin temeli olarak bilinir. T2 çipe sahip Mac bilgisayarlarda macOS güvenli başlatmanın güvenilirliği T2 çiple başlar. (Hem T2 çip hem de Secure Enclave kendi ayrı başlatma ROM'larını kullanarak kendi güvenli başlatma süreçlerini uygular. A serisi ve M1 çipler de güvenli başlatma sürecini tıpkı bu şekilde gerçekleştirir.)

Secure Enclave ayrıca Apple aygıtlarındaki Touch ID ve Face ID sensörlerinden gelen parmak izi ve yüz verilerini de işler. Bu sayede kimlik doğrulama işlemi güvenli bir şekilde yapılabilir ve kullanıcıların biyometrik verileri gizli ve güvende tutulur. Ayrıca kullanıcılar daha uzun ve karmaşık parolaların sağladığı güvenlikten ve birçok durumda erişim veya alışveriş için gereken hızlı kimlik doğrulama kolaylığından yararlanır.

Apple aygıtlarındaki bu güvenlik özellikleri yalnızca Apple'ın sunduğu çip tasarımı, donanım, yazılım ve hizmetlerin birleşimiyle mümkündür.

Sistem güvenliği
Apple donanımlarının benzersiz yeteneklerini temel alan sistem güvenliği, kolay kullanımdan ödün vermeden Apple aygıtlarındaki sistem kaynaklarına erişimi denetleme sorumluluğu taşıyor. Sistem güvenliği; başlatma sürecini, yazılım güncellemelerini ve CPU, bellek, disk, program yazılımları ve depolanan veriler gibi bilgisayardaki sistem kaynaklarının korunmasını kapsıyor.

Apple işletim sistemlerinin en yeni sürümleri en güvenli olanlardır. Sistemi başlatma sırasında kötü amaçlı yazılımlardan koruyan güvenli başlatma, Apple güvenliğinin önemli bir kısmını oluşturur. Güvenli başlatma donanımda başlar ve yazılım yoluyla bir güven zinciri oluşturur. Bu zincirde her adım, kontrolü devretmeden önce bir sonraki adımın doğru bir şekilde çalışıp çalışmadığını kontrol eder. Bu güvenlik modeli yalnızca Apple aygıtlarının varsayılan başlatma yöntemini değil çeşitli kurtarma modlarını ve Apple aygıtlarındaki düzenli güncellemeleri de destekler. T2 çip ve Secure Enclave gibi alt bileşenler kendi güvenli başlatma işlemlerini gerçekleştirerek Apple'dan gelen doğru kodların haricinde kod çalıştırmamasını sağlar. Güncelleme sistemi sürüm düşürme saldırılarını bile önleyebilir. Böylece aygıtlar, kullanıcı verilerini çalmak için işletim sisteminin (zayıf noktaları saldırganlar tarafından bilinen) daha eski bir sürümüne geri döndürülemez.

Başlatma ve çalıştırma korumaları da içeren Apple aygıtları devam eden işlemler boyunca bütünlüklerini koruyabilir. iPhone, iPad, Apple Watch, Apple TV ve HomePod'daki Apple tasarımı çip ile Apple çipine sahip Mac, işletim sistemi bütünlüğünü korumak için ortak bir mimari sunar. macOS, tüm Mac donanım platformlarında desteklenen özelliklerin yanı sıra kendi farklı bilgi işlem modelini destekleyen genişletilmiş ve yapılandırılabilir koruma özelliklerine de sahiptir.

Şifreleme ve veri koruması
Apple aygıtlarında kullanıcı verilerini korumak için şifreleme özellikleri bulunur ve aygıtın çalınması veya kaybolması durumunda verileri uzaktan silmek mümkündür.

Güvenli başlatma zinciri, sistem güvenliği ve uygulama güvenliği özellikleri aygıt üzerinde yalnızca güvenilen kodların ve uygulamaların çalıştığını doğrulamaya yardımcı olur. Apple aygıtları, güvenlik altyapısının diğer bileşenleri ele geçirilmiş olsa bile (örneğin aygıtın kaybolması veya güvenilmeyen kodları çalıştırması durumunda) ek şifreleme özellikleriyle kullanıcı verilerini korur. Tüm bu özellikler, kişisel ve kurumsal bilgileri koruyarak ve aygıtın çalınması ya da kaybolması durumunda tüm verileri anında uzaktan silmeyi sağlayan yöntemler sunarak hem kullanıcılara hem IT yöneticilerine fayda sağlar.

iOS ve iPadOS aygıtları, Veri Koruma adı verilen bir dosya şifreleme yöntemi kullanır. Intel tabanlı Mac'ler ise FileVault adı verilen bir birim şifreleme teknolojisiyle korunur. Apple çipe sahip Mac'ler, Veri Koruma özelliğini destekleyen hibrit bir model kullanır. Bu modelde dikkat edilmesi gereken iki nokta vardır: En düşük koruma düzeyi (D sınıfı) desteklenmez ve varsayılan düzey (C sınıfı) bir birim anahtarı kullanarak tıpkı Intel tabanlı Mac'lerdeki FileVault gibi çalışır. Her durumda, anahtar yönetimi hiyerarşilerinin kökü Secure Enclave'ın özel çipinde yer alır. Hat hızında şifrelemeyi destekleyen özel AES motoru, uzun ömürlü şifreleme anahtarlarının (ele geçirilmeye açık hale gelebilecekleri) çekirdek işletim sistemine veya CPU'ya gösterilmemesine yardımcı olur. (T1 çipe sahip veya Secure Enclave'e sahip olmayan Intel tabanlı Mac'ler, FileVault şifreleme anahtarlarını korumak için özel bir çip kullanmaz.)

Verilere yetkisiz erişimi önlemeye yarayan Veri Koruma ve FileVault'un yanı sıra, Apple'ın işletim sistemi çekirdekleri de koruma ve güvenliği güçlendirir. Çekirdek, uygulamaları izole ederek erişebilecekleri verileri sınırlayan erişim denetimlerinden ve Data Vault adı verilen bir mekanizmadan yararlanır. Data Vault, bir uygulamanın yapabileceği çağrıları kısıtlamak yerine diğer uygulamaların talep ettikleri uygulama verilerine erişimini kısıtlar.

Uygulama güvenliği

Uygulamalar, güvenlik mimarisinin en kritik öğeleri arasında yer alır. Uygulamalar, kullanıcılar için olağanüstü üretkenlik avantajları sağlasa da doğru şekilde kullanılmadıklarında sistem güvenliğini, stabil çalışmayı ve kullanıcı verilerini olumsuz etkileyebilir.

Bu nedenle Apple, uygulamaların bilinen kötü amaçlı yazılımları içermediğinden ve uygulamalara müdahale edilmediğinden emin olmaya yardımcı olan birçok koruma katmanı sunuyor. Uygulamaların kullanıcı verilerine erişiminin dikkatli bir şekilde düzenlenmesini sağlayan ek koruma yöntemleri de bulunuyor. Bu güvenlik denetimleri uygulamalar için stabil ve güvenli bir platform sağlayarak, binlerce geliştiricinin sistem bütünlüğünü etkilemeden iOS, iPadOS ve macOS için yüz binlerce uygulama sunmasına olanak verir. Kullanıcılar Apple aygıtlarında virüs, kötü amaçlı yazılım veya yetkisiz saldırılar konusunda endişelenmeden bu uygulamalara erişebilir.

En sıkı denetimi sağlamak için iPhone, iPad ve iPod touch'taki tüm uygulamalar App Store'dan indirilir ve tümü izole bir şekilde çalışır.

Mac'te birçok uygulama App Store'dan indirilir ancak Mac kullanıcıları internetten de uygulama indirip kullanabilir. macOS internetten indirmeyi güvenli bir şekilde desteklemek için ek denetim katmanları sunar. Öncelikle, macOS 10.15 ve daha yeni sürümlerinde varsayılan olarak tüm Mac uygulamalarının açılmadan önce Apple tarafından onaylanması gerekir. Bu gereklilik, uygulamaların App Store

üzerinden indirilmeseler bile bilinen kötü amaçlı yazılımları içermediklerini doğrulamaya yardımcı olur. Ayrıca, macOS kötü amaçlı yazılımları engellemek ve gerekirse silmek için en gelişmiş antivirüs korumasını sağlar.

Platformlarda ek denetim sağlayan uygulama izolasyonu, kullanıcı verilerini uygulamaların yetkisiz erişimine karşı korumaya yardımcı olur. macOS'te kritik alanlardaki veriler özel olarak korunur. Bu sayede erişim talebinde bulunan uygulamalar izole olmasa bile Masaüstü, Belgeler, İndirilenler ve diğer alanlardaki dosyalara erişim kullanıcının kontrolü altında olur.

Hizmet güvenliği

Apple, kullanıcıların aygıtlarından daha fazla fayda ve üretkenlik sağlamalarına yardımcı olmak için bir dizi güçlü hizmet geliştirdi. Bu hizmetler bulutta depolama, eşzamanlama, parola depolama, kimlik doğrulama, ödeme, mesajlaşma, iletişim ve daha fazlası için güçlü özellikler sunarken kullanıcı gizliliğini ve verilerin güvenliğini korur.

Bu hizmetler arasında iCloud, Apple ile Giriş Yap, Apple Pay, iMessage, Business Chat, FaceTime, Bul ve Süreklilik yer alıyor. Hizmetlerden yararlanmak için Apple ID veya Yönetilen Apple ID gerekebilir. Bazı durumlarda Yönetilen Apple ID, Apple Pay gibi belirli hizmetlerle kullanılamayabilir.

Not: Tüm Apple hizmetleri ve içerikleri her ülkede veya bölgede mevcut değildir.

Ağ güvenliğine genel bakış

Apple'ın Apple aygıtlarında depolanan verileri korumak için kullandığı yerleşik koruma önlemlerine ek olarak, kuruluşların bir aygıta giden veya aygıttan gelen bilgileri güvende tutmak için alabileceği birçok önlem vardır. Tüm bu korumalar ve önlemler ağ güvenliği başlığı altında toplanır.

Kullanıcıların dünyanın her yerinden kurumsal ağlara erişebilmesi gerekir. Bu nedenle, yetkilerinin doğrulanması ve aktarım sırasında verilerinin korunması önem kazanıyor. Bu güvenlik hedeflerine ulaşmak için iOS, iPadOS ve macOS'te hem Wi-Fi hem de hücresel veri ağı bağlantıları için kanıtlanmış teknolojiler ve en yeni standartlar kullanılır. İşte bu yüzden işletim sistemlerimizde kimlik doğrulaması yapılmış, yetkilendirilmiş ve şifrelenmiş iletişimler için standart ağ protokolleri kullanılır ve geliştiricilerin de bu protokollere erişebilmesi sağlanır.

Apple aygıtları ve güvenlik hakkında daha fazla bilgi edinin.

apple.com/tr/business/it

apple.com/tr/macos/security

apple.com/tr/privacy/features

apple.com/security

İş ortağı ekosistemi

Apple aygıtları, ortak kurumsal güvenlik araçları ve hizmetleriyle çalışarak aygıtların ve aygıtlardaki verilerin uyumlu olmasını sağlar. Her platform, ağ trafiğini korumak amacıyla iOS ve iPadOS 14'te hesap başına VPN bağlantıları dahil VPN ve güvenli Wi-Fi için standart protokolleri destekler. Bu platformlar ortak kurumsal altyapılara da güvenli bir şekilde bağlanır.

Apple'ın Cisco ile kurduğu iş ortaklığı, gelişmiş güvenlik ve üretkenlik sağlıyor. Cisco ağları, Cisco Security Connector aracılığıyla gelişmiş güvenlik sağlar. Cisco ağlarında iş uygulamalarına öncelik verilir.