

Akıllı Telefonlar için Antivirüs Uygulamaları: Faydalı mı Yoksa Gereksiz Bir Koruma mı?

Mobil uç noktalar olarak akıllı telefonlar ve tabletler, saldırganlara şirket ağlarına giriş kapısı sunar. Bu nedenle birçok kişi antivirüs ya da güvenlik uygulamalarına yönelir. E-kitabımızda, bunların kullanmaya değer olup olmadığını öğrenebilirsiniz.

Akıllı telefonlar ve tabletler için antivirüs uygulamaları nasıl çalışır?

Akıllı telefonlar için antivirüs uygulamaları, bilgisayarlardaki antivirüs programlarına benzer şekilde çalışır; ancak **Android** veya **iOS** gibi mobil işletim sistemlerinin özel özelliklerine uyarlanmıştır.



Akıllı telefonlardaki antivirüs uygulamalarının temel özellikleri şunlardır:

Kötü amaçlı yazılımları tarama

- Uygulama, yüklü uygulamaları, dosyaları ve indirmeleri bilinen virüsler, truva atları, casus yazılımlar, reklam yazılımları veya fidye yazılımlarına karşı tarama.
- Android'de özellikle uygulama kodları (APK dosyaları) taranır, çünkü Android'de üçüncü taraf sağlayıcılardan uygulama yüklemek mümkündür.
- iOS ise bu konuda çok daha kısıtlayıcıdır, bu nedenle kötü amaçlı yazılım taramaları burada daha az önemlidir (aşağıya bakınız).

Akıllı telefonlardaki antivirüs uygulamalarının temel özellikleri:

2. Gerçek zamanlı koruma

- Birçok antivirüs uygulaması, yeni indirilen dosyaları veya uygulama kurulumlarını otomatik olarak kontrol eden arka plan koruması sunar.
- Bazı uygulamalar ayrıca, gezinti yaparken tehlikeli web sitelerinin erişilip erişilmediğini kontrol eder (kimlik avı koruması).

3. Güvenlik özellikleri (çoğunlukla ek ücretli ek özellikler)

- Hırsızlık koruması (yer tespiti, uzaktan kilitleme, hırsızlık durumunda veri silme).
- Güvenli gezinti için VPN.
- Belirli uygulamaları PIN veya parmak izi ile ek güvenlik sağlamak için uygulama kilidi.
- Güvensiz ağları tespit etmek için WiFi güvenlik kontrolü.

Android vs. iOS: Fonksiyonellikteki Farklar

Android

- Antivirüs uygulamaları, Android'in daha fazla özgürlük tanınması nedeniyle sisteme derinlemesine müdahale edebilir.
- Bu nedenle, özellikle **resmi olmayan** kaynaklardan (Play Store dışı) uygulama yüklediğinizde bir virüs tarayıcısı burada faydalıdır.

iOS

- Apple, antivirüs uygulamalarının sistem dosyalarına veya diğer uygulamalara erişmesine izin vermez, bu yüzden gerçek virüs tarayıcıları iPhone'larda klasik anlamda çalışmaz.
- iOS antivirüs uygulamaları genellikle sadece güvenlik ipuçları, veri koruma raporları veya tarayıcıda kimlik avı uyarıları sunar - başka bir deyişle, virüs korumasından çok daha fazla "güvenlik tavsiyesi" sağlar.



Akıllı telefonlardaki antivirüs uygulamaları ne kadar faydalı?

Antivirüs uygulamaları, zaten yüklü olan uygulamaları tarayabilir ve tehlikeli indirmeler veya web siteleri hakkında uyarılarda bulunabilir. Bu nedenle, belirli bir koruma seviyesi sunarlar. Ancak, bu koruma şirketler için yeterli değildir çünkü GDPR'nin sıkı gereksinimlerine uymaları gerekir. Güvenlik uygulamalarının ne yapabileceğini ve hangi bağlamda kullanılmaları gerektiğini her zaman göz önünde bulundurmak önemlidir. **Bu nedenle, bir mobil güvenlik uygulamasının cihazları güvence altına almak için tek çözüm olarak kullanılması tavsiye edilmez.**



Akıllı telefonlardaki antivirüs uygulamaları ne kadar faydalı?



Kurumsal bağlamda, antivirüs uygulamaları bu nedenle yalnızca MDM (mobil cihaz yönetimi) yazılımı gibi **sıkı, önleyici önlemlerin** bir tamamlayıcısı olabilir. Antivirüs ve güvenlik uygulamalarının bir diğer yönü ise, son kullanıcıların güvenlik hissini artırabilmesidir. Özellikle teknoloji kullanımı konusunda kararsız olan kişiler için, bu uygulamalar mobil cihazları iş için kullanırken **daha rahat hissetmelerine** yardımcı olabilir. Antivirüs uygulamaları aracılığıyla gelen uyarılar, son kullanıcıların dikkatsiz davranmalarını engelleyebilir. Ayrıca, **potansiyel tehditlere karşı farkındalık** da artırılabilir.

Virüsler, kötü amaçlı yazılımlar ve saldırılara karşı MDM ve güvenlik uygulamaları ile kapsamlı güvenlik

Prensip olarak, antivirüs ve güvenlik uygulamalarının ek olarak kullanılması, şirketin güvenliğine zarar vermez ve mobil cihazların güvenliğine katkı sağlayabilir. Dahası, MDM kullanımı çoğu şirket için zorunludur. Bunun nedeni, yalnızca bir MDM aracılığıyla şirket mobil cihazlarında kapsamlı güvenlik önlemleri alınabilmesidir. Örneğin, yönergeler belirli uygulamaların indirilmesini engeller veya yetkisiz WiFi bağlantılarının kullanılmasını yasaklar.

BT yöneticisi, bir MDM kullanarak yalnızca şirketin uyum yönergelerine uyan uygulamaların listelendiği bir uygulama kataloğu oluşturabilir. Bu, cihazlarda son kullanıcı verilerine çok fazla erişim gerektiren uygulamaların kullanılmamasını sağlar. Güvenlik özelliklerine ek olarak, MDM, cihaz yönetimini de basitleştirir; örneğin, uygulamaların uzaktan yüklenmesine, işletim sisteminin otomatik olarak güncellenmesine veya duvar kağıtlarının merkezi olarak dağıtılmasına olanak tanır.



MDM ve antivirüs uygulamaları nasıl yardımcı olabilir?

SMS kimlik avı

- Bir MDM, belirli telefon numaralarını yasaklayabilir, örneğin 0800 numaralarını.
- Gelen metin mesajları MDM aracılığıyla engellenebilir.
- Bir antivirüs uygulaması, metin mesajlarındaki şüpheli bağlantıları tespit edebilir.

Üçüncü taraf kaynaklardan uygulama yükleme (yan yükleme)

- Bir MDM, uygulamaların Play Store ve App Store dışından indirilmesini engelleyebilir.
- Eğer buna izin verilirse, bir antivirüs uygulaması, uygulama dosyasını indirme sırasında tarayabilir ve kötü amaçlı yazılım hakkında uyarı verebilir.

Veri güvenliği

- Bir MDM yardımıyla, cihazlar iki alana ayrılabilir: özel profil ve iş profili, bu da önemli verilerin temiz bir şekilde ayrılmasını sağlar.
- Bir güvenlik uygulaması, belgeler, resimler ve diğer dosyalar paylaşılırken ve gönderilirken alıcının şüpheli görünüp görünmediğini de belirtebilir.

MDM ve antivirüs uygulamaları nasıl yardımcı olabilir?

İnternet bağlantısının güvenliğini sağlama

- Bir MDM, WiFi bağlantılarının kullanılmadan önce hangi güvenlik standartlarını karşılaması gerektiğini belirleyebilir.
- Şirket dışındaki WiFi bağlantıları tamamen engellenebilir.
- Bir antivirüs uygulaması, WiFi bağlantılarını tarayarak güvenlik risklerine dikkat çekebilir.

Güvenli iletişim

- Bir MDM, özel ve iş alanları arasında dosya paylaşımını engelleyebilir.
- MDM, GDPR'ye uygun güvenli mesajlaşma uygulamalarını yüklemek için kullanılabilir.

Şifrelerin ve cihaza erişimin korunması

- Bir MDM, şifre gereksinimleri belirleyebilir; bu gereksinimler karşılanmazsa cihaz kullanılamaz.
- Bir güvenlik uygulaması, şifrelerin güvenli bir şekilde saklanmasını sağlayabilir.

Yazarlar hakkında

IOTIQ GmbH, Almanya'nın Leipzig şehrinde bulunan uluslararası bir BT şirketidir. 2017 yılından bu yana özellikle KOBİ'ler için özelleştirilmiş yazılım çözümleri sunmaktayız.

Amacımız: Almanya'da dijitalleşmeyi hızlandırmak - en iyi yazılımla, akıllı telefonunuz için. Tüm büyüklükteki şirketlerin dijitalleşmenin avantajlarından faydalanabilmesi gerektiğine inanıyoruz: İhtiyaca özel uygulama geliştirmeden donanım danışmanlığı ve tedarikine kadar. Mobil cihazların dijital ilerlemenin anahtarı olduğuna inanıyoruz.

Bu makalenin yazarı, IOTIQ GmbH'de Müşteri Hizmetleri ve Pazarlama Müdürü olup, sertifikalı bir Android uzmanıdır.



Android
Enterprise

Silver partner