

► KASPERSKY SECURITY FOR MOBILE

Tüm mobil uç noktalar için çok katmanlı güvenlik, yönetim ve kontrol

Mobil cihazlar gün geçtikçe siber suçlulara daha çekici gelmektedir. Bununla birlikte, "Kendi Cihazını Getir" (BYOD) yaklaşımı cihaz yelpazesini daha çeşitli ve karmaşık hale getirerek, BT yöneticileri için zorlu bir yönetim ve kontrol ortamı ortaya çıkarmaktadır.

Kaspersky Security for Mobile cihazınızın her yerde güvende olmasını sağlar. Sürekli gelişen kötü amaçlı mobil yazılımlara karşı koruma sağlar. Ortamınızdaki akıllı telefonlar ve tabletler üzerinde tek bir merkezi konumdan ve minimum müdahale ile hızlı ve kolay görünürlük ve kontrol sağlar.

- Güçlü Kötü Amaçlı Yazılımdan Koruma
- Kimlik Avı Koruması ve Anti-Spam
- Web koruması
- Uygulama Kontrolü
- Rooting/jailbreak algılaması
- Konteynerizasyon
- Hırsızlığa karşı koruma
- Mobil Cihaz Yönetimi
- Self Servis Portal
- Merkezi yönetim
- Web Konsolu
- Desteklenen platformlar:
 - Android™
 - iOS
 - Windows Phone

ÖNE ÇIKAN NOKTALAR

MOBİL CİHAZLAR İÇİN GELİŞMİŞ KÖTÜ AMAÇLI YAZILIMDAN KORUMA VE VERİ GÜVENLİĞİ

Kaspersky Lab, sadece 2014 yılında yaklaşık 1,4 milyon benzersiz kötü amaçlı mobil saldırıyı önledi. Kaspersky Security for Mobile, mobil cihazlarda saklanan verileri bilinen ve bilinmeyen tehditlere karşı koruyan kötü amaçlı yazılım önleme ve derin koruma teknolojisi katmanlarını bir arada kullanır.

MOBİL CİHAZ YÖNETİMİ (MDM)

Tüm lider mobil cihaz yönetim platformlarıyla entegrasyon, Android, iOS ve Windows Phone cihazlarının daha kolay kullanılabilmesi ve yönetilebilmesi için uzaktan "Kablosuz" (OTA) dağıtım ve kontrol olanağı sağlar.

MOBİL UYGULAMA YÖNETİMİ (MAM)

Konteynerizasyon ve seçmeli silme olanakları, aynı cihazda işletme verileri ve kişisel verilerin ayrılmasına olanak sağlayarak BYOD girişimlerini destekler. Şifreleme işlevimiz ve kötü amaçlı yazılımdan koruma teknolojimizle birlikte kullanılan Kaspersky Security for Mobile, cihazı ve verilerini yalıtarak korumayı deneyen basit bir çözüm değil, bir proaktif mobil koruma çözümdür.

MERKEZİ YÖNETİM

Birden fazla platform ve cihazı aynı konsoldan farklı uç noktalar olarak yönetin. Bu platform, daha fazla çaba veya teknoloji yönetimi gereksinimi ortaya çıkarmadan görünürlüğü ve kontrolü artırır.

MOBİL GÜVENLİK VE YÖNETİM ÖZELLİKLERİ

GÜÇLÜ KÖTÜ AMAÇLI YAZILIMDAN KORUMA

İmza tabanlı, proaktif ve bulut destekli (Kaspersky Security Network - KSN ile) koruma, bilinen ve bilinmeyen kötü amaçlı mobil tehditlere karşı koruma sağlar. İsteğe bağlı ve planlı taramalar ve otomatik güncellemeler koruma düzeyini artırır.

KİMLİK AVI KORUMASI VE ANTI-SPAM

Güçlü Kimlik Avı Koruması ve Anti-Spam teknolojileri, cihazı ve verileri kimlik avı saldırılarına karşı korur ve istenmeyen çağrı ve mesajların filtrelenmesine yardımcı olur.

WEB KONTROLÜ/SAFE BROWSER

Kaspersky Security Network (KSN) tarafından desteklenen bu teknolojiler, kötü amaçlı ve izinsiz kullanımı hedefleyen web sitelerinin erişimini engellemek için gerçek zamanlı olarak çalışırlar. Safe Browser sürekli güncellenen itibar analizi sunarak güvenli mobil gezinme sağlar.

UYGULAMA KONTROLÜ

KSN ile entegre edilen Uygulama Kontrolü, uygulamanın sadece onaylı yazılımı kullanmasını sağlayarak belirsiz veya izinsiz yazılımların kullanılmasını önler. Cihaz işlevini gerekli uygulamaların yüklenmesine bağlı hale getirir. Uygulama etkin olmama kontrolü, yöneticilerin uygulamaların belirli bir süre boyunca kullanılmadığı durumlar için yeniden oturum açmayı zorunlu kılmasına olanak sağlar. Bu yaklaşım cihaz kaybolduğunda veya çalındığında uygulama açık olsa bile verilerin korunmasını sağlar.

ROOTING/JAILBREAK ALGILAMASI

Rooting veya jailbreak işlemlerini otomatik algılama ve raporlama, konteynerlere erişimi otomatik engelleme, seçmeli silme veya tüm cihazı silme özellikleriyle takip edilebilir.

KONTEYNERİZASYON

Uygulamaları konteynerlerde "paketleyerek" işletme verilerini ve kişisel verileri birbirinden ayırın. Hassas verileri korumak için şifreleme gibi ek ilkeler uygulanabilir. Seçmeli silme, işletmeden ayrılan çalışanın cihazında konteynerde saklanan verilerin çalışanın kişisel verilerine dokunmadan silinmesine olanak sağlar.

HIRSIZLIĞA KARŞI KORUMA

Silme, cihazı kilitleme, konum belirleme, SIM izleme, "gizli fotoğraf çekme" ve "alarm" cihazı algılama gibi uzaktan Hırsızlığa Karşı Koruma özellikleri, cihazın kaybolduğu ya da çalındığı durumlarda etkinleştirilebilir. Hırsızlığa karşı koruma komutları, duruma bağlı olarak oldukça esnek bir şekilde uygulanabilir. Örneğin, Google Cloud Messaging (GCM) entegrasyonu komutların anında iletilmesini sağlar, yanıt sürelerini kısaltır ve güvenliğe katkıda bulunur. Ayrıca komutların Self-Service Portal ile gönderilmesi yöneticilerin eyleme geçmesi zorunluluğunu ortadan kaldırır.

MOBİL CİHAZ YÖNETİMİ (MDM)

Microsoft Exchange ActiveSync, Apple MDM ve Samsung KNOX 2.0 desteği, geniş bir ilke kapsamını birleşik bir arabirimle ve platformdan bağımsız olarak etkinleştirir. Örn. şifreleme ve parola uygulama veya kamera kullanımı kontrol etme, bireysel kullanıcılar ya da gruplara ilkeler uygulama, APN/VPN ayarlarını yönetme vb.

SELF SERVİS PORTAL

Rutin güvenlik yönetiminin çalışanlara dağıtılması, onaylı cihazların otomatik kaydedilmesini sağlar. Yeni cihaz etkinleştirme sürecinde tüm gerekli sertifikalar, yönetici müdahalesine gerek olmadan portal üzerinden otomatik olarak gönderilebilir. Cihazın kaybolması durumunda, çalışan tüm mevcut Hırsızlığa Karşı Koruma eylemlerini Portal yoluyla uygulayabilir.

MERKEZİ YÖNETİM

Tüm mobil cihazları, aynı zamanda tüm diğer uç noktaların BT güvenliğinin yönetilmesine olanak sağlayan tek bir konsoldan merkezi olarak yönetin. Web Konsolu, yöneticilerin cihazları tüm bilgisayarlardan uzaktan kontrol etmelerine ve yönetmelerine olanak sağlar.

Satın alma

Kaspersky Security for Mobile şunlarla birlikte verilir:

- Kaspersky Endpoint Security for Business – Select
- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

Kaspersky Security for Mobile, Hedeflenmiş bir Çözüm olarak ayrıca satın alınabilir.

Ayrıntılı bilgi ve fiyatlar için bayinizle iletişime geçin.