TREND MICRO™

Securing Your Journey to the Cloud

MOBİL CİHAZ ENTEGRASYONUNU (CONSUMERIZATION) BENİMSEYİN. FIRSATI AÇIĞA ÇIKARIN.

Bugün kuruluşlardaki en önemli eğilimlerden biri, bilgi teknolojilerinin Mobil Cihaz Entegrasyonudur (Consumerization). BT'nin demokratikleşmesi günümüz kullanıcılarının teknik konularda daha önce hiç olmadığı kadar deneyimli oldukları ve kişisel BT tercihlerinin iş ve özel yaşamlarına sızdığı anlamına gelir. Kullanıcılar ilişkilerini Facebook üzerinden sürdürüyor, Dropbox ile dosyalarına her yerden erişiyor ve Google Apps ve Wikis gibi birlikte çalıştıkları uygulamaları ve bilgileri etkin bir şekilde biçimlendirme özgürlüğüne sahip olmaya alıştılar. Sonuç olarak, kullanıcılar artık "bağlantılı" bir yaşam sürüyor ve birçok durumda kişisel BT ekipmanları, Internet bağlantıları, akıllı telefonlarının veri planları, işverenlerinin onlara sunduklarından çok daha iyi. Artı, kullanıcılar bu cihazları kendileri tercih edip seçtiği için, kendi cihazlarını kullanma konusundaki motivasyonları artmış durumda.

Bunu şimdi iş piyasasına giren kendilerine ait kişisel BT ve her zaman her yerde kullanabildikleri Internet bağlantısı olmayan bir dünyayı bilmeyen genç profesyoneller olarak bilinen "Yeni Bin Yıl" nesli ile bir araya getirdiğinizde, bu yeni yetenek dalgasını kendisine çekmek ve elinde tutmak amacıyla, şirketlerin bu yeni nesile işlerini yapmak için standart dizüstü bilgisayarlardan daha cazip BT varlıkları sunmak zorunda oldukları çok açıktır.

Kuruluşlar Açısından Mobil Cihaz Entegrasyonunun Zorlukları

Mobil Cihaz Entegrasyonunu benimseyen organizasyonların kendilerini ve şirketlerini riske maruz bırakmamak, veri kaybı yaşamamak ve itibarlarını kaybetmemek için özellikle dikkatli olmaları gerekir. Ancak, Mobil Cihaz Entegrasyonunu benimserken aşağıdaki zorlukların üstesinden gelmek, önemli bir fırsatın ortaya çıkmasını sağlayabilir:

Kullanıcının sorumlu olduğu muazzam cihaz çeşitliliğini yönetme ve koruma

Kurumların "Kendi Cihazını Getir" (ya da KCG) programlarına sponsor olup olmamasına ya da kullanıcının sahip ya da sorumlu olduğu cihazların kurumsal ağ üzerinde kullanılmasına izin verip vermemesine bakılmaksızın, cihazların kurumsal BT erişim kurumsal kaynakları tarafından kontrol edilmiyor olması, aşağıdaki kaygılara neden olmaktadır:

- Cihazın ağ kaynaklarıma erişmesi güvenli mi ya da cihaz kullanıcılar ve veri merkezi genelinde yıkıma yol açabilecek kötü niyetli yazılım ya da arka kapılara neden olarak kurumsal BT'nin güvenliği açısından bir tehdit teşkil ediyor mu?
- Cihaz kaybolur ya da çalınırsa, veriler ve kurumsal verilere erişim bilgileri güvende olacak mı?
- Kullanıcılar ve BT operasyonları (desteği) kullanıcı ya da destek sorunlarına neden olmadan, nasıl bu cihazların ağ üzerinde kolayca kullanılmasını sağlayacak?
- Herhangi bir performans sınırı olduğu varsayılamazsa, kuruluşlar kullanıcının sahip olduğu bilgisayarları nasıl koruyacak?

Kuruluşun Sosyal Ortamı benimseme ve uygulamaları internet üzerinde çalıştırma süreçlerini koruma

Kullanıcılar uygulamalara her yerden eriştiği ve iletişim için sosyal ortam, forumlar ve Wiki'lerden faydalanmaya alıştıkları için, her geçen gün daha çok sayıda kuruluş bu teknolojileri iş amaçlarına yönelik olarak da benimsemektedir. Bu süreçte, şunlardan emin olmaları gerekir:

- Müşteri web uygulamaları güvenlidir ve suistimal edilemez
- İşbirliği uygulamaları zararlı içerik barındırmaz ya da yaymaz
- Kuruluşlar bulut bilgi işlem sistemini benimsedikçe, hassas kurumsal bilgiler riske maruz kalmaz

Sürekli görülebilirliği ve kontrolü sürdürme

Cihaz, işletim sistemi, veri planı ve kullanıcı davranışı çeşitliliğine bağlı olarak, görülebilirliği yitiren kuruluşlar bir anda kendilerini riske maruz kalmış halde bulurlar; çünkü görülebilirlik yeni BT paradigmasını etkili bir şekilde korumanın 1 numaralı ön koşuludur. Cihazların ve kullanıcıların yerini saptamak, iletişim modellerini izlemek ve şüpheli etkinliği kesin olarak saptamak makul derecede güvenli bir ortamdaki mutlu ve üretken kullanıcılar ile BT anarşisi, kaosu ve patlayan maliyetler arasındaki farkı belirleyecektir.

Trend Micro nasıl yardımcı olabilir?

Mobil Cihaz Entegrasyonu geniş kapsamlı ve hızla büyüyen bir olgudur. Doğal olarak, Mobil Cihaz Entegrasyonunun tüm zorluklarını hedef alan tek bir sihirli ürün olamaz. Cihazlarını, ağlarını ve verilerini gereksiz risklere maruz bırakmadan, müşterilerin BT operasyonlarını dönüştürmelerine yardımcı olacak şekilde tasarlanan kapsamlı ve entegre çözümler portföyü sunan Trend Micro kuruluşları ve bulut sistemine uzanan yolculuklarını koruma altına alan lider kuruluşlardan biridir.

Mobil Cihaz Yönetimi ve Mobil Cihaz Güvenliği. Neredeyse tüm mobil işletim sistemleri için kullanılabilen ve “en güncel” tehdit bilgileri için bulut güvenliğinden faydalanan Trend Micro Mobile Security Android, BlackBerry OS ve Apple iOS de dahil olmak üzere, akıllı telefonları ve tabletleri yönetir ve korur.

Sektörün en az yer kaplayan ama en hızlı ve en etkili tehdit koruması seti sayesinde, Az Yer Kaplayan ve Performans Üzerinde Az Etki Yaratan Uç Nokta Güvenliği bilgisayar ve Mac uç noktaları korur.

Veri koruması sadece şifrelemeden çok daha fazlasıdır. Trend Micro ister sabit, ister hareketli, ister kullanımda olsun, veriler için uçtan uca koruma sağlamak için uç nokta, sunucu ve ağ katmanında gerçek içerik bilinçliliği ile güçlü veri şifreleme teknolojisini (en yeni kendi kendini şifreleyen sabit diskler de dahil olmak üzere) bir araya getirir.

Web ve bulut sisteminde kurumsal uygulamalar. Müşterileri Sunucu Sanallaştırmasından Masaüstü Sanallaştırmasına ve bulut bilgi işlem sistemine uzanan yolculuğa çıkaran ve bu yolcuk süresince kullanıcıları koruyan, uygulamaları koruma altına alan ve kurumsal bilgiler ile uygulamaların gizliliğini ve bütünlüğünü sürdüren güvenlik çözümleri sağlayan Trend Micro sanallaştırma ve bulut güvenliğinde 1 numaralı satıcıdır.

Tehdit Keşfi ve Tehdit Bilgileri Yönetimi. Tüm kullanıcıları ve cihazları onaylamak, Mobil Cihaz Entegrasyonu Yapılmış BT ortamlarında gerçekleştirilmesi mümkün bir yaklaşım değildir. Trend Micro’nun izinsiz araya girmeyen, bant dışı himaye teknolojisi sahte cihazları belirler ve tehlikeli ya da zararlı akışı saptar ve böylelikle, yöneticiler kontrolü ele alabilirler.