Microsoft 365 ile Zero Trust Güvenlik Modeli

Günümüzde siber saldırılara karşı etkili önlemler almamız gerekiyor. Özellikle Supply Chain Attack gibi saldırı türlerinde önlem almak karmaşık ve zor duruma gelmekteydi. Yaşanan zaafiyet ve vakalar sonrası Zero Trust Modeli etkili ve önemli bir güvenlik yaklaşımı olarak karşımıza çıktı.

Zero Trust Modeli ele alındığı zaman bir ürün bir yazılım gibi algı oluşabiliyor. Ancak Zero Trust yaygın kanının aksine bir güvenlik yaklaşımıdır. Zero Trust Modeli, Kurumsal Firewall'ların arkasında dahi hiçbir şeyin güvenli olmadığını varsaymaktadır. Bu nedenle her isteği açık erişimli bir ağdan geliyormuşçasına inceleyerek her bağlantıya sıfır tolerans uygulamaktadır.

Talebin nereden geldiği, hangi kaynağa yönelik olduğu önemli değil. "**Hiçbir zaman güvenme, her zaman kontrol et**" anlayışına sahiptir.

Zero Trust Güvenlik Modeli'nde gelen bir talebe erişim isteği verilmeden önce isteğin tamamen doğrulanması, yetkilendirilmesi ve şifrelenmesi önemlidir. Ayrıca olası yaşanan anormal durumlarda gerçek zamanlı olarak tespit ve çözüm odaklı hareket ederek, sisteme entegre bileşenler ile sistem güvenliğini en üst düzeyde tutmaktadır.

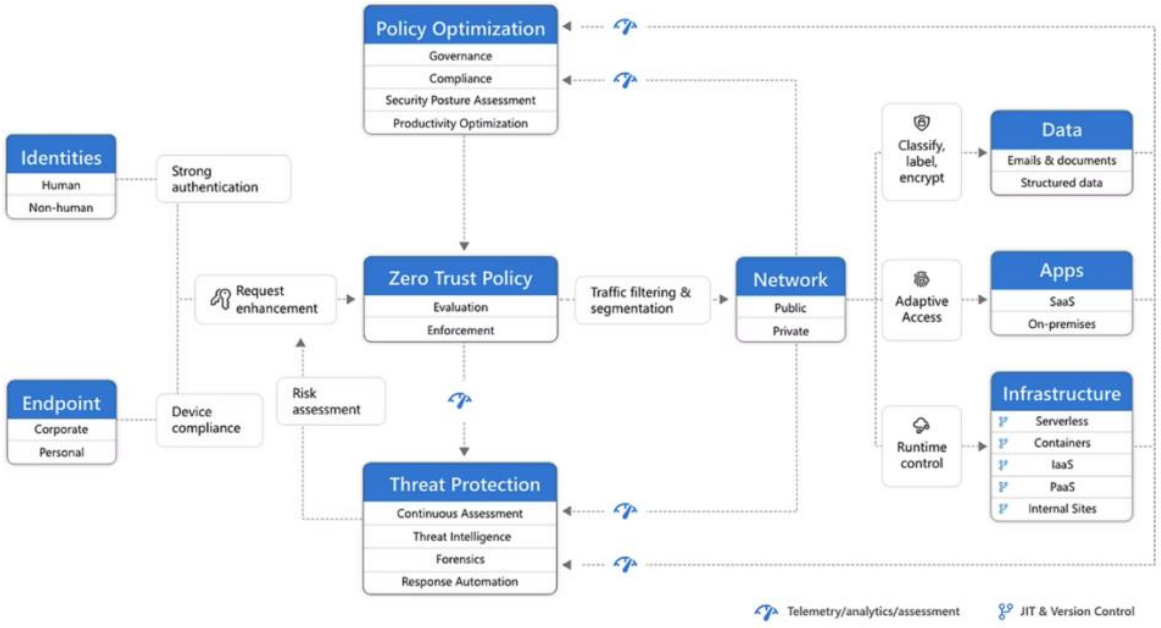
Zero Trust Modeli, günümüzde yaygınlaşan mobil kullanımı , kimlik güvenliğini, cihaz ve uygulama güvenliğini sağlayan, verileri platform bağımlılığı olmadan uyum sağlayacak şekilde çalışmalıdır.

Şirketlerimizde kurgulanacak olan yapıda, Zero Trust Modelini oluşturan adımlara dikkat etmeli ve altyapıya entegre çalışacak olan siber güvenlik çözümlerinde bu koşulların yer alıp sağlanabileceğini özellikle dikkat etmek gerekir.

Microsoft ile Zero Trust Güvenlik duruşunuzun ne seviyede olduğunu görmek için aşağıdaki bağlantıdan testi çözebilirsiniz.

Güvenlik Duruşu Testi

Microsoft Zero Trust Mimarisi

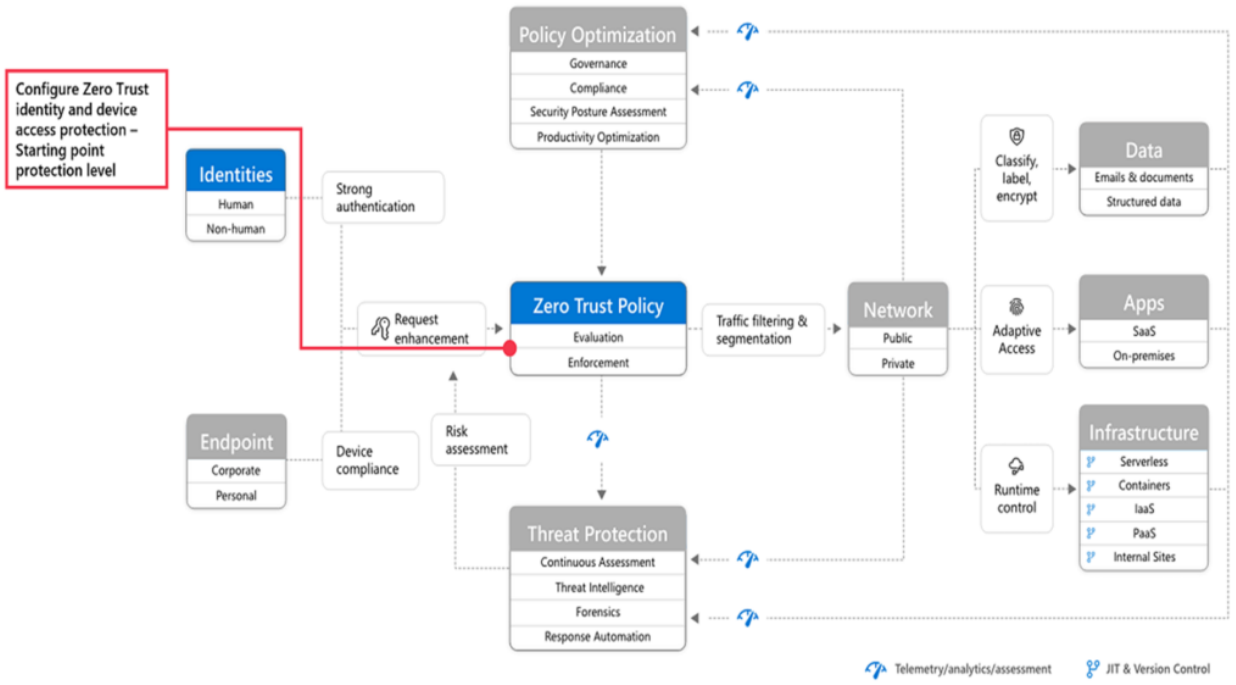


Mirosoft Zero Trust Mimarisi'nde;

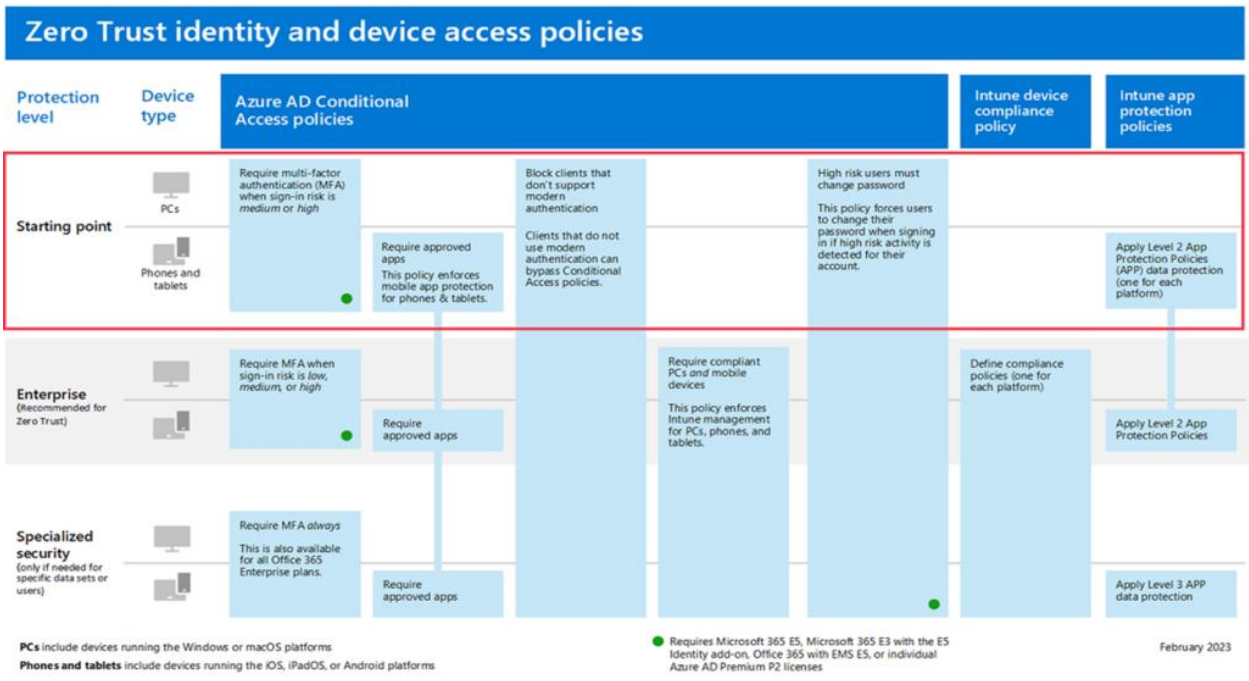
- Güvenlik politikaları Zero Trust mimarisinin merkezinde yer almaktadır. Böylece kullanıcı hesabı riskini, cihaz durumunu ve belirlediğiniz kriterleri ve politikaları dikkate alan koşullu erişime sahip MFA'i içerir.
- Kimlikler, cihazlar, veriler, uygulamalar, ağ ve diğer altyapı bileşenlerinin tamamı uygun güvenlikle yapılandırılmıştır. Bu bileşenlerin her biri için yapılandırılan politikalar genel Zero Trust stratejinizle koordine edilir. Örneğin, cihaz politikaları sağlıklı cihazlara ilişkin kriterleri belirler ve koşullu erişim politikaları, belirli uygulamalara ve verilere erişim için tehdit barındırmayan cihazların kullanılması gerekir.
- Ayrıca Threat Protection and intelligence tüm ortamı izlemektedir. Ortamda oluşan tüm riskleri çıkarır ve gelen ataklar için otomatik düzeltme eylemlerini devreye almaktadır.
-

Microsoft Zero Trust Dağıtım Planını kısaca incelediğimizde;

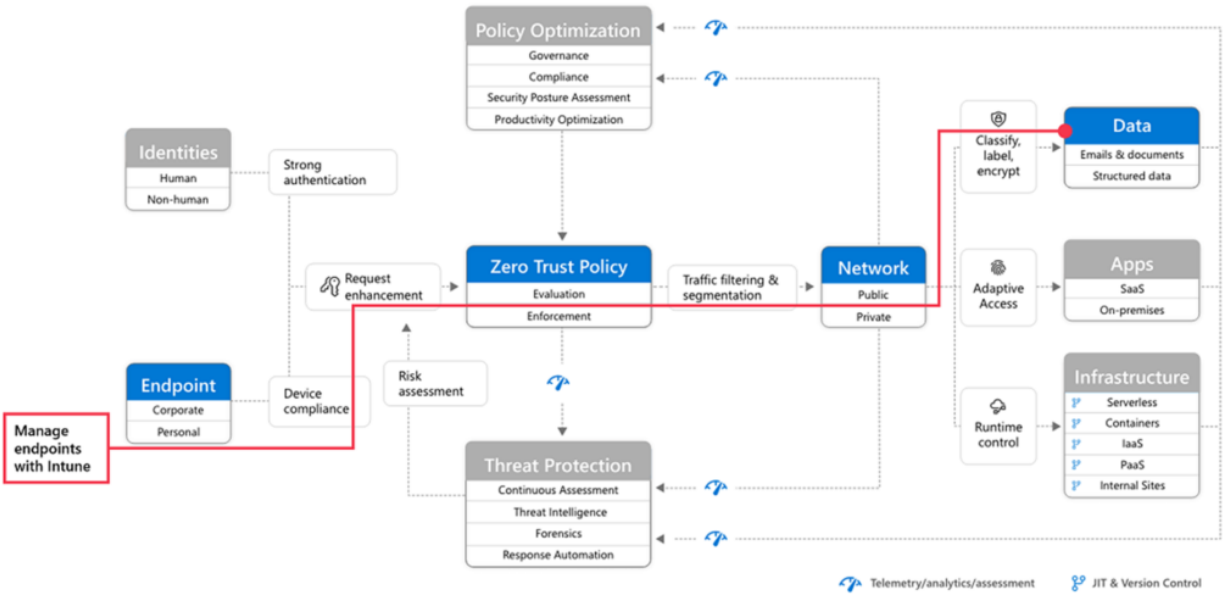
Adım 1: Zero Trust Kimlik ve Cihaz Erişim Koruması'nın Yapılandırılması



Atılacak olan ilk adım, kimlik ve cihaz erişim korumasını devreye alarak Zero Trust temelini oluşturmaktadır.

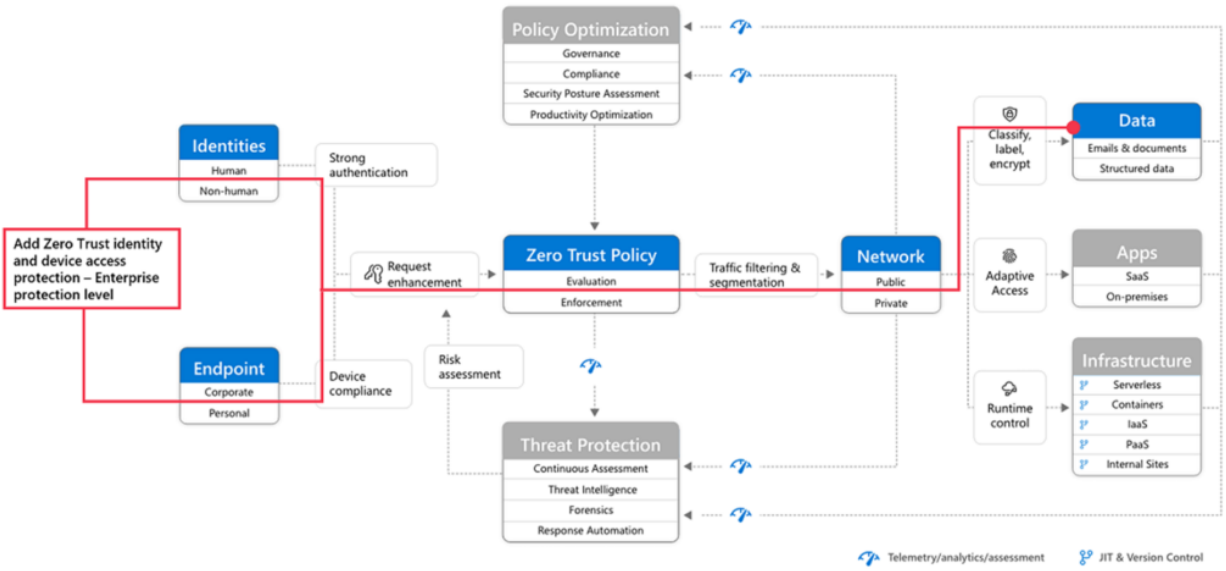


Adım 2: Intune ile Endpoint Cihazların Yönetimi

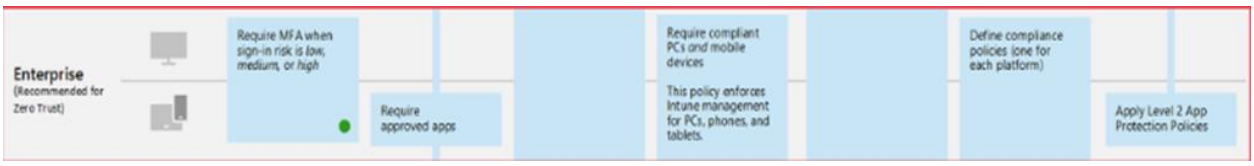


Kimlik ve cihaz erişim korumasını devreye aldıktan sonra bir sonraki adım olarak cihazlarımızı Endpoint Management yapısına dahil ederek daha gelişmiş kontrollerle korumaya başlayabiliriz

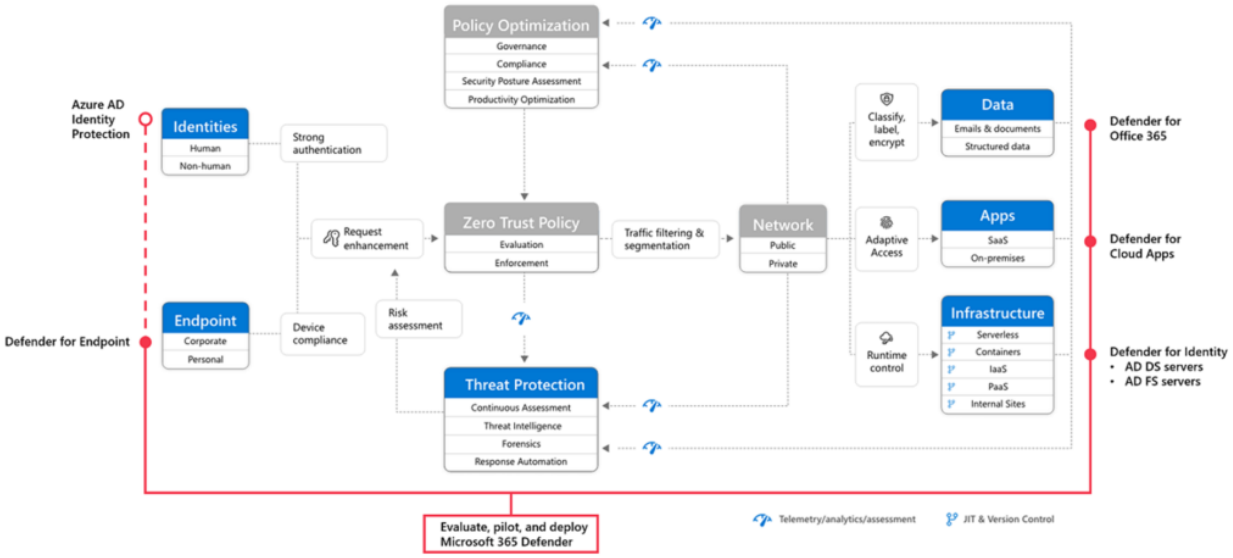
Adım 3: Zero Trust Kimlik ve Cihaz Erişim Koruması Politikalarının Eklenmesi



Cihazlarımızı Endpoint Management ile yönetebilir durumda olduğumuzda kimlik ve cihaz erişim politikalarının tamamını uygulayabiliriz.

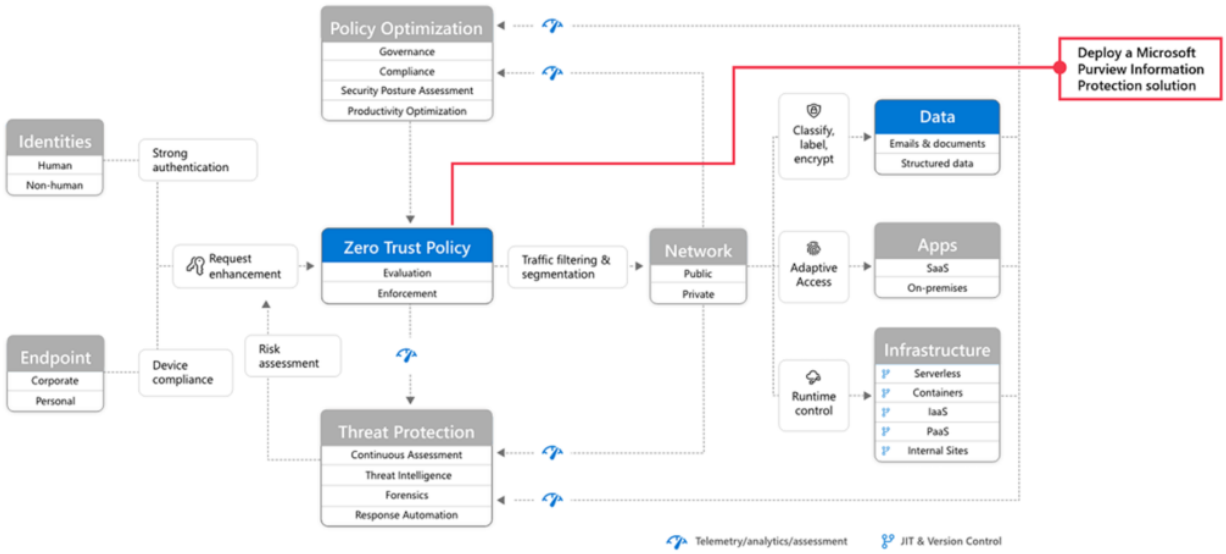


Adım 4: Microsoft 365 Defender ile Pilot Uygulamalar ve Dağıtım



Microsoft 365 Defender, endpoint, e-posta, uygulamalar ve kimlikler de dahil olmak üzere Microsoft 365 ortamınızdaki sinyal, tehdit ve uyarı verilerini otomatik olarak toplar, ilişkilendirir ve analiz doğrultusunda çözüme kavuşturur. Bu yaklaşım çerçevesinde inceleme, pilot uygulamalar ve dağıtım aşamaları gerçekleştirilebilir.

Adım 5: Hassas Verilerin Korunması ve Yönetimi



Son olarak, Microsoft Purview ile, hassas bilgilerimiz nerede olursa olsun korunmasına olanak sağlar. Verilerinizi tanımanıza, korumanıza ve veri kaybını önlemenize olanak sağlacaktır.

M365 Zero Trust Detaylı Dağıtım Planına linke tıklayarak ulaşabilirsiniz.