

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 şifrenmesi 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.

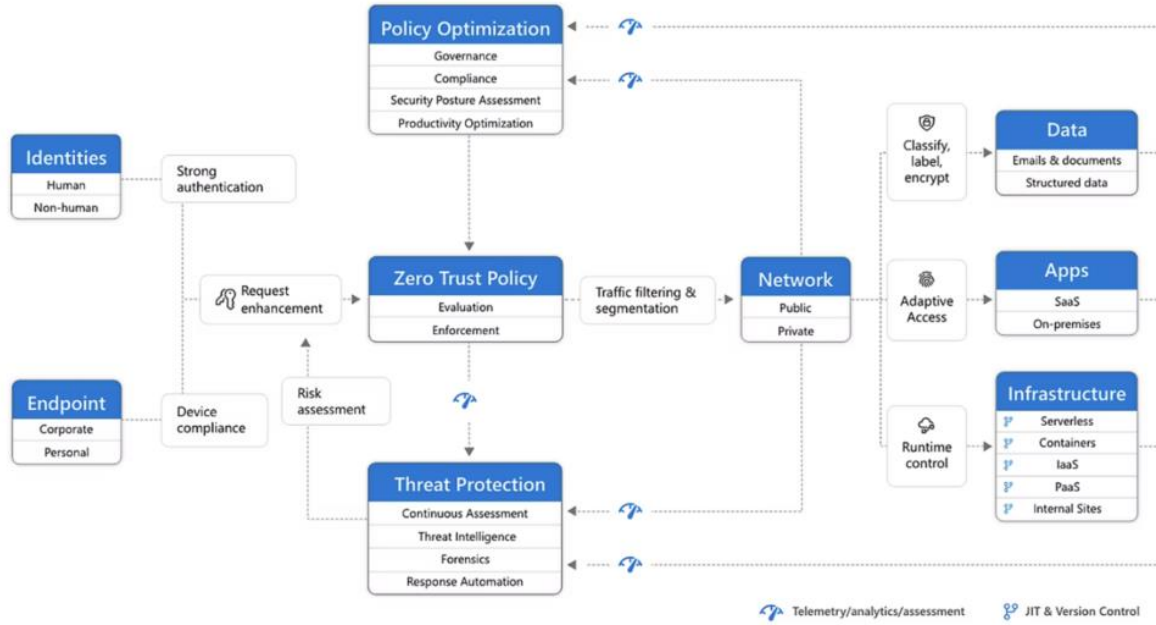
Zero Trust Modeli, günümüzde yaygınlaşan mobil kullanımı , kimlik güvenliğini, cihaz ve uygulama güvenliğini sağlayan, verileri platform bağımlılığı olmadan uyum sağlayacak şekilde çalışmalıdır.

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

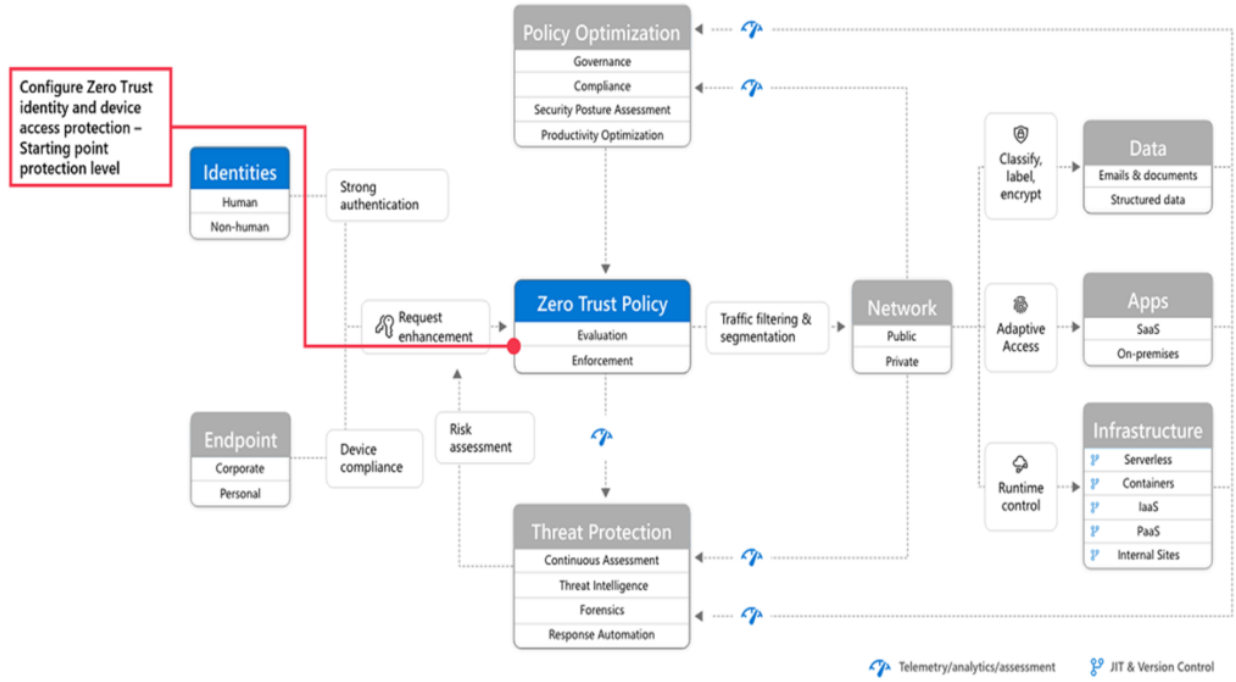


Microsoft Zero Trust Mimarisi'nde;

- 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'ı 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.

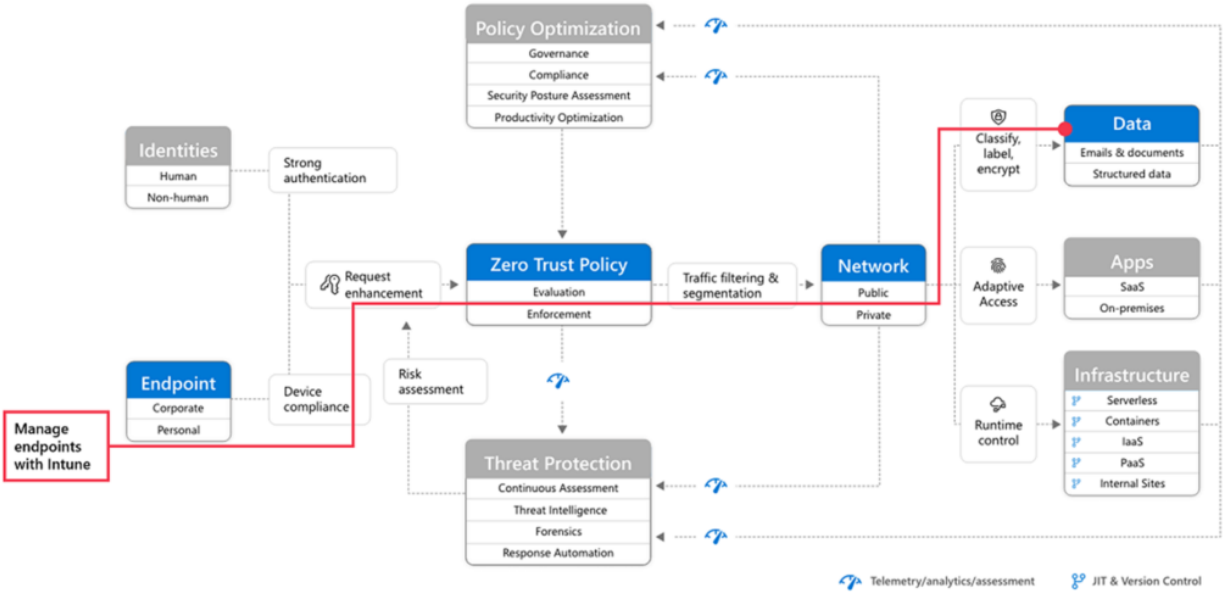
Zero Trust identity and device access policies					
Protection level	Device type	Azure AD Conditional Access policies		Intune device compliance policy	Intune app protection policies
Starting point	PCs	Require multi-factor authentication (MFA) when sign-in risk is medium or high	Block clients that don't support modern authentication	High risk users must change password This policy forces users to change their password when signing in if high risk activity is detected for their account.	Apply Level 2 App Protection Policies (APP) data protection (one for each platform)
	Phones and tablets	Require approved apps This policy enforces mobile app protection for phones & tablets.	Clients that do not use modern authentication can bypass Conditional Access policies.		
Enterprise (Recommended for Zero Trust)	PCs	Require MFA when sign-in risk is low, medium, or high	Require compliant PCs and mobile devices This policy enforces Intune management for PCs, phones, and tablets.	Define compliance policies (one for each platform)	Apply Level 2 App Protection Policies
Specialized security (only if needed for specific data sets or users)	PCs	Require MFA always This is also available for all Office 365 Enterprise plans.			Apply Level 3 APP data protection

PCs include devices running the Windows or macOS platforms
Phones and tablets include devices running the iOS, iPadOS, or Android platforms

● Requires Microsoft 365 E5, Microsoft 365 E3 with the E5 Identity add-on, Office 365 with EMS E5, or individual Azure AD Premium P2 licenses

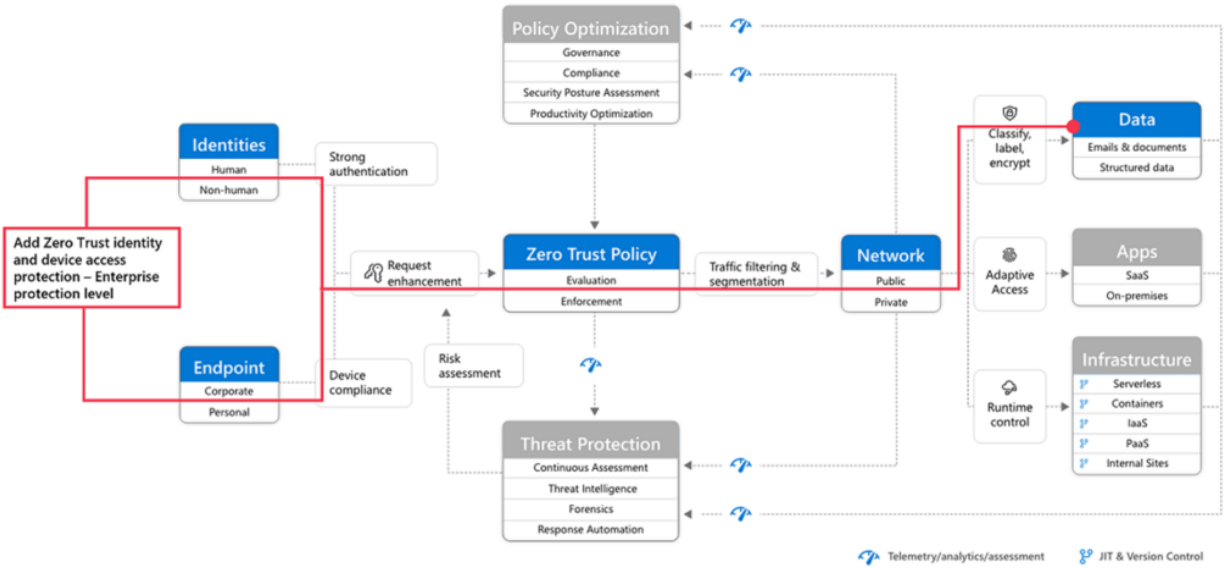
February 2023

Adım 2: Intune ile Cihazların Yönetimi

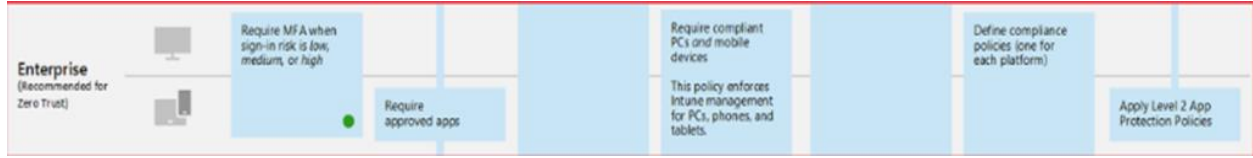


Kimlik ve cihaz erişim korumasını devreye aldıktan sonra bir sonraki adım olarak cihazlarımızı Endpoint Management yapısına dahil ederek daha gelişmiş kontrollerle korumaya başlayabiliriz

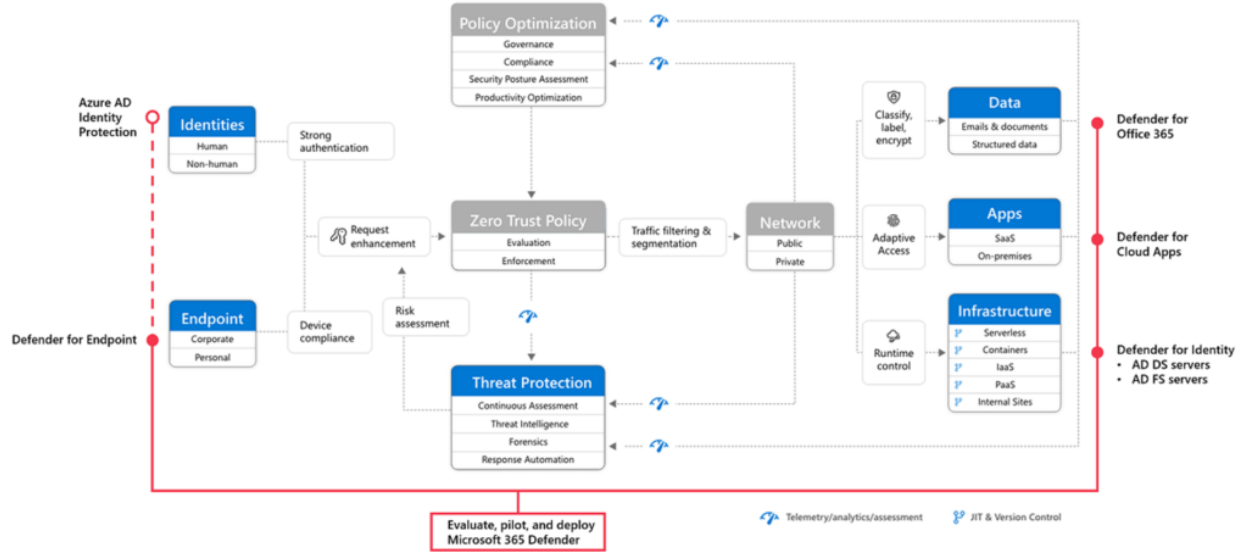
Adım 3: Zero Trust Kimlik ve Cihaz Erişim Koruması Politikalarının Eklenmesi



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

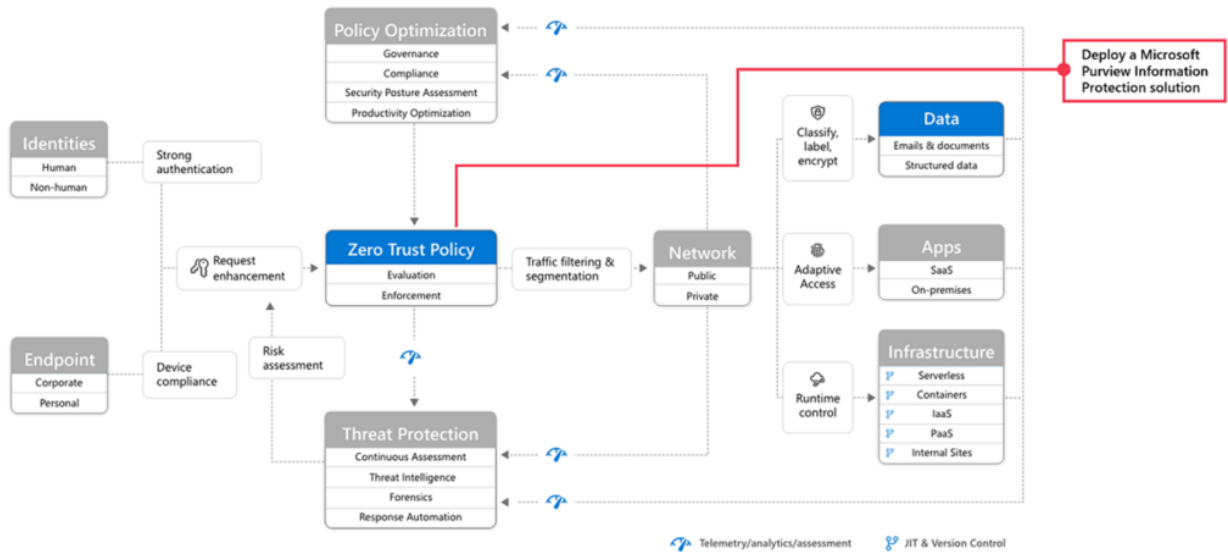


Adım 4: Microsoft 365 Defender ile Pilot Uygulamalar ve Dağıtım



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 sağlayacaktır.

[M365 Zero Trust Detaylı Dağıtım Planına linke tıklayarak ulaşabilirsiniz.](#)