

Zero Trust Security Model with Microsoft 365

Nowadays, we need to take effective measures against cyber attacks. It was becoming complicated and difficult to take precautions, especially in attack types such as Supply Chain Attack. After the vulnerabilities and incidents, the Zero Trust Model emerged as an effective and important security approach.

When the Zero Trust Model is considered, a product can be perceived as a software. However, contrary to popular belief, Zero Trust is a security approach. The Zero Trust Model assumes that nothing is secure, even behind Corporate Firewalls. Therefore, it examines every request as if it were coming from an open access network and applies zero tolerance to every connection.

It doesn't matter where the demand comes from or to which source it is directed. He has a " never trust, always check " mentality.

In the Zero Trust Security Model, it is important that the request is fully verified, authorized and encrypted before granting an access request. In addition, it acts with a real-time detection and solution focus in possible abnormal situations and keeps system security at the highest level with the components integrated into the system.

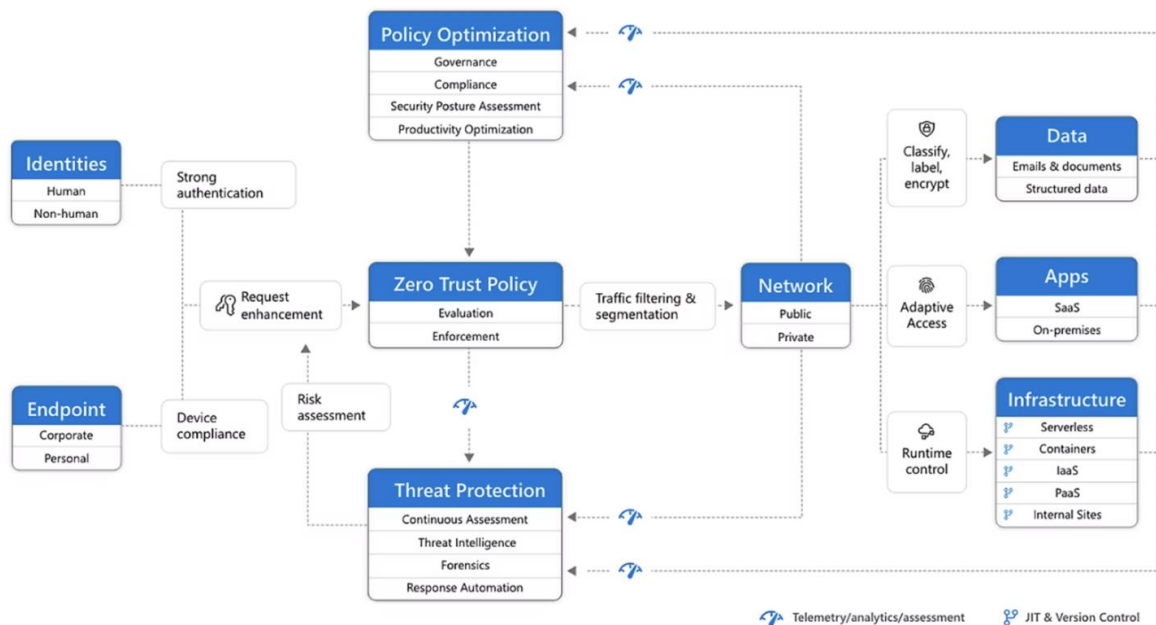
The Zero Trust Model should work in a way that ensures identity security, device and application security, and adapts data without platform dependency to today's widespread mobile use.

In the structure to be established in our companies, we should pay attention to the steps that form the Zero Trust Model and pay particular attention to whether these conditions can be included and met in cyber security solutions that will work integrated with the infrastructure.

Zero Trust with Microsoft You can take the test from the link below to see what level your security posture is.

[Safety Posture Test](#)

Microsoft Zero Trust Architecture



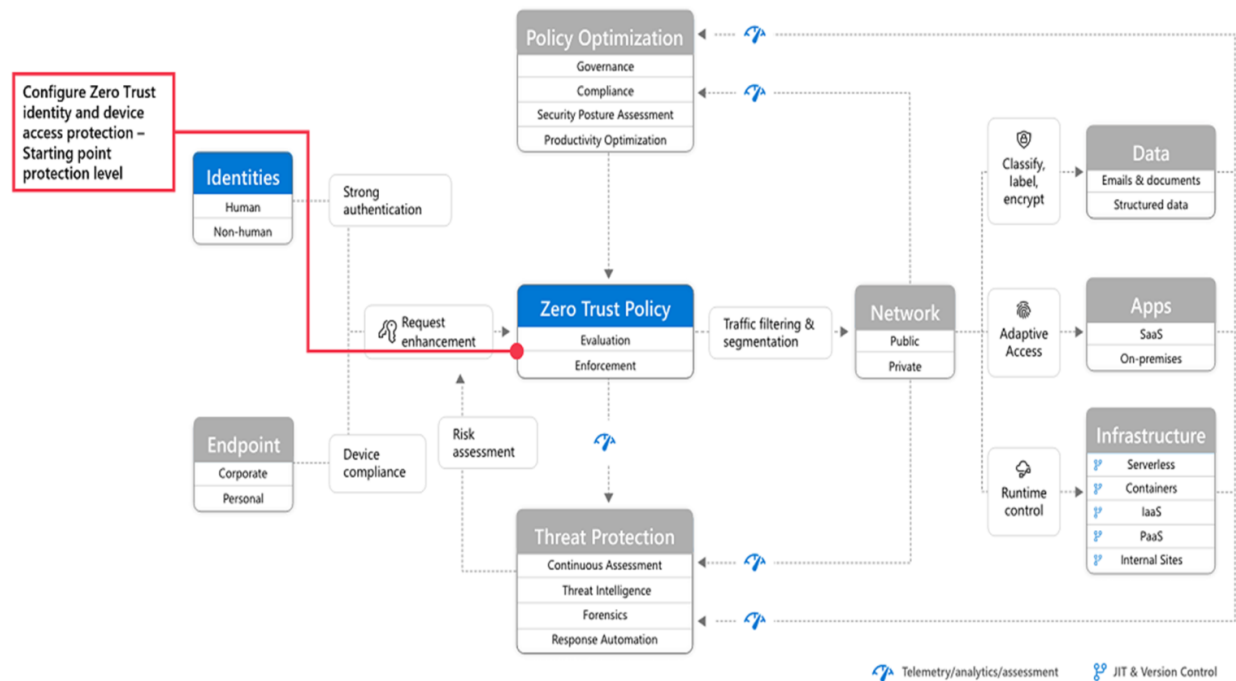
In Microsoft Zero Trust Architecture;

Security policies are at the heart of Zero Trust architecture. This includes MFA with conditional access, which takes into account user account risk, device health, and the criteria and policies you set. Identities, devices, data, applications, network and other infrastructure components are all configured with appropriate security. The policies configured for each of these components are coordinated with your overall Zero Trust strategy. For example, device policies set criteria for healthy devices, and conditional access policies require threat-free devices to access certain applications and data.

Additionally, Threat Protection and intelligence monitors the entire environment. It removes all risks occurring in the environment and activates automatic correction actions for incoming attacks.

When we briefly examine the Microsoft Zero Trust Distribution Plan;

Step 1: Configuring Zero Trust Identity and Device Access Protection



The first step to be taken is to establish the foundation of Zero Trust by activating identity and device access protection.

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.		
	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 <small>(Recommended for Zero Trust)</small>	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
	Phones and tablets	Require approved apps				
Specialized security <small>(only if needed for specific data sets or users)</small>	PCs	Require MFA always This is also available for all Office 365 Enterprise plans.	Require compliant PCs and mobile devices This policy enforces Intune management for PCs, phones, and tablets.			Apply Level 3 APP data protection
	Phones and tablets	Require approved apps				

PCs include devices running the Windows or macOS platforms

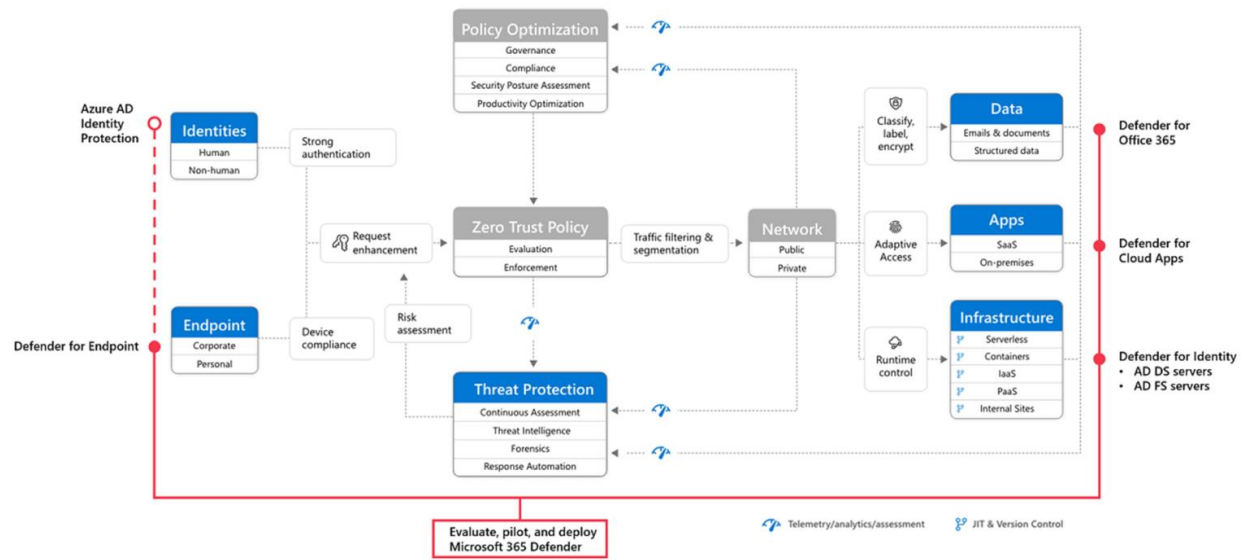
Phones and tablets include devices running the iOS, iPadOS, or Android platforms

● 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

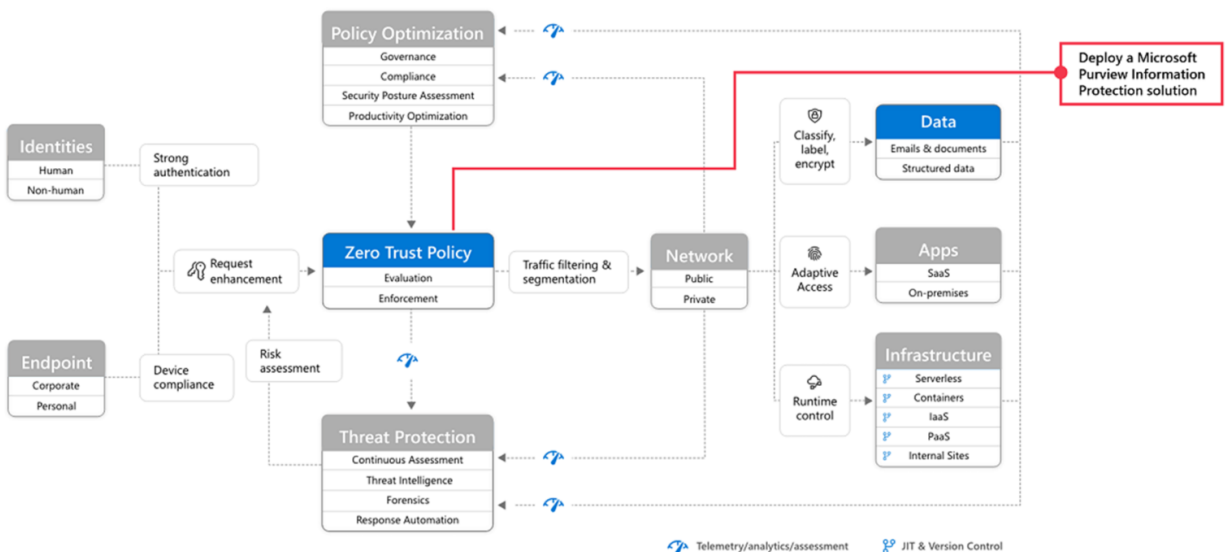
Step 2: Managing Endpoint Devices with Intune

Step 4: Pilots and Deployment with Microsoft 365 Defender



Microsoft 365 Defender automatically collects, correlates and analyzes signal, threat and alert data in your Microsoft 365 environment, including endpoints, email, applications and identities. Within the framework of this approach, review, pilot applications and distribution stages can be carried out.

Step 5: Protection and Management of Sensitive Data



Finally, with Microsoft Purview, our sensitive information is protected no matter where it is located. It will allow you to recognize and protect your data and prevent data loss.

[You can access the M365 Zero Trust Detailed Distribution Plan by clicking the link.](#)