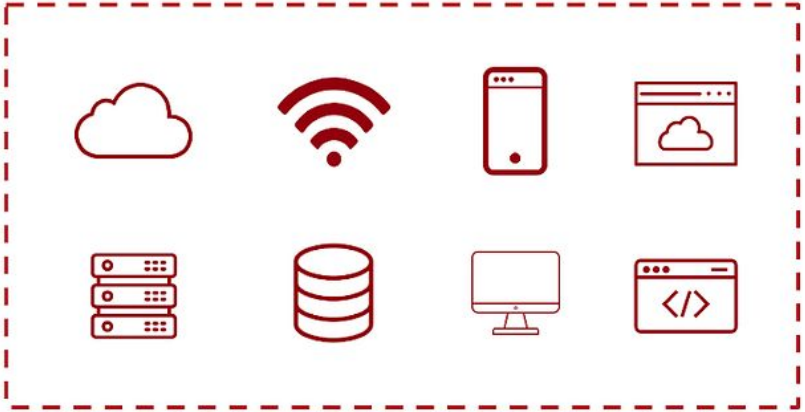
Zero Trust Architecture

Shifting from Perimeter to Perimeter-less Security

Traditional Security

Where are you coming from?

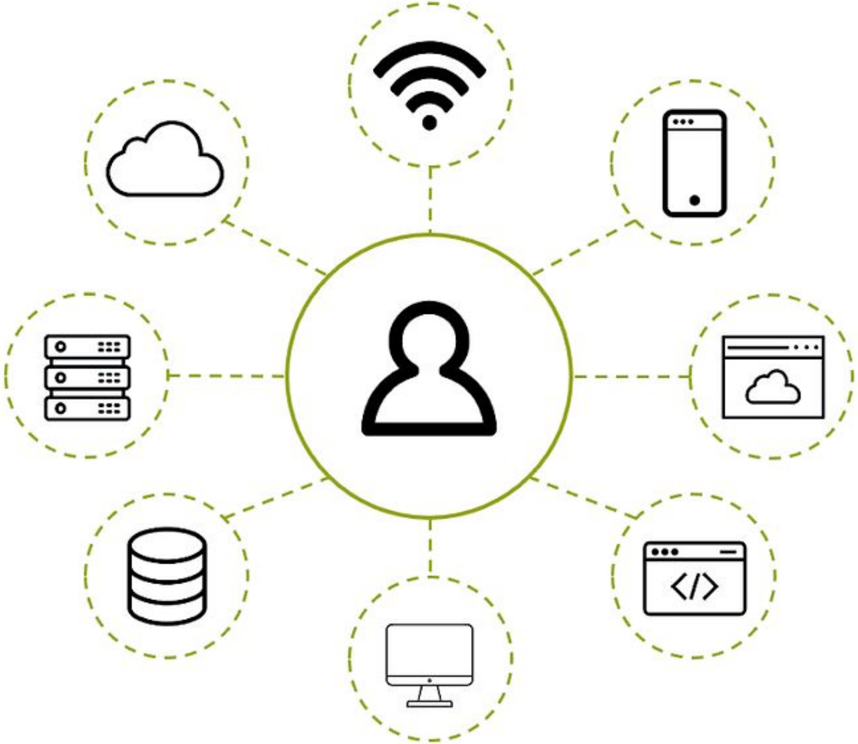


Perimeter ("Traditional") Security:

- Relies on on-premise firewalls and VPNs to restrict access to a **"secure"** network
- **Internal Trust:** Devices within the network perimeter are trusted by default
- **External Distrust:** Users and devices outside the network perimeter are untrusted.

Zero Trust

Who are you?



Issues with Perimeter Security

Rise in remote work
How do we make sure people are who they say they are?

Rise in Cloud Services
How do we secure our network when the attack surface expands beyond traditional boundaries and data can be accessed from anywhere?

User-Owned Devices
How do we make sure devices are secure and free from malware?

Easy for lateral movement
After compromising one endpoint, an attacker can easily gain access to other resources on the network.

Why Zero Trust?

- **“Trust nothing, verify everything”**
- Requires all users, whether inside or outside the network, to be authenticated, authorized, and continuously validated
- Emphasizes strict access control and **never trusts implicitly***

*There is the “implicit trust zone” where an entity is **briefly** trusted in order to access a **specific** resource.*

Zero Trust Principles

Verify Explicitly	• Strict, **continuous identity verification** for every user and device accessing resources, **regardless of its origin** within the corporate network or whether it has previously accessed this resource
Least Privilege	• Grant **minimal access necessary** for specific tasks • Use Just-In-Time (JIT) and Just-Enough-Access (JEA) principles
Assume Breach	• Operate under the assumption that **attackers are already inside the network**. • Real-time monitoring • deny-all approach • access segregation

How do we enforce these principles?

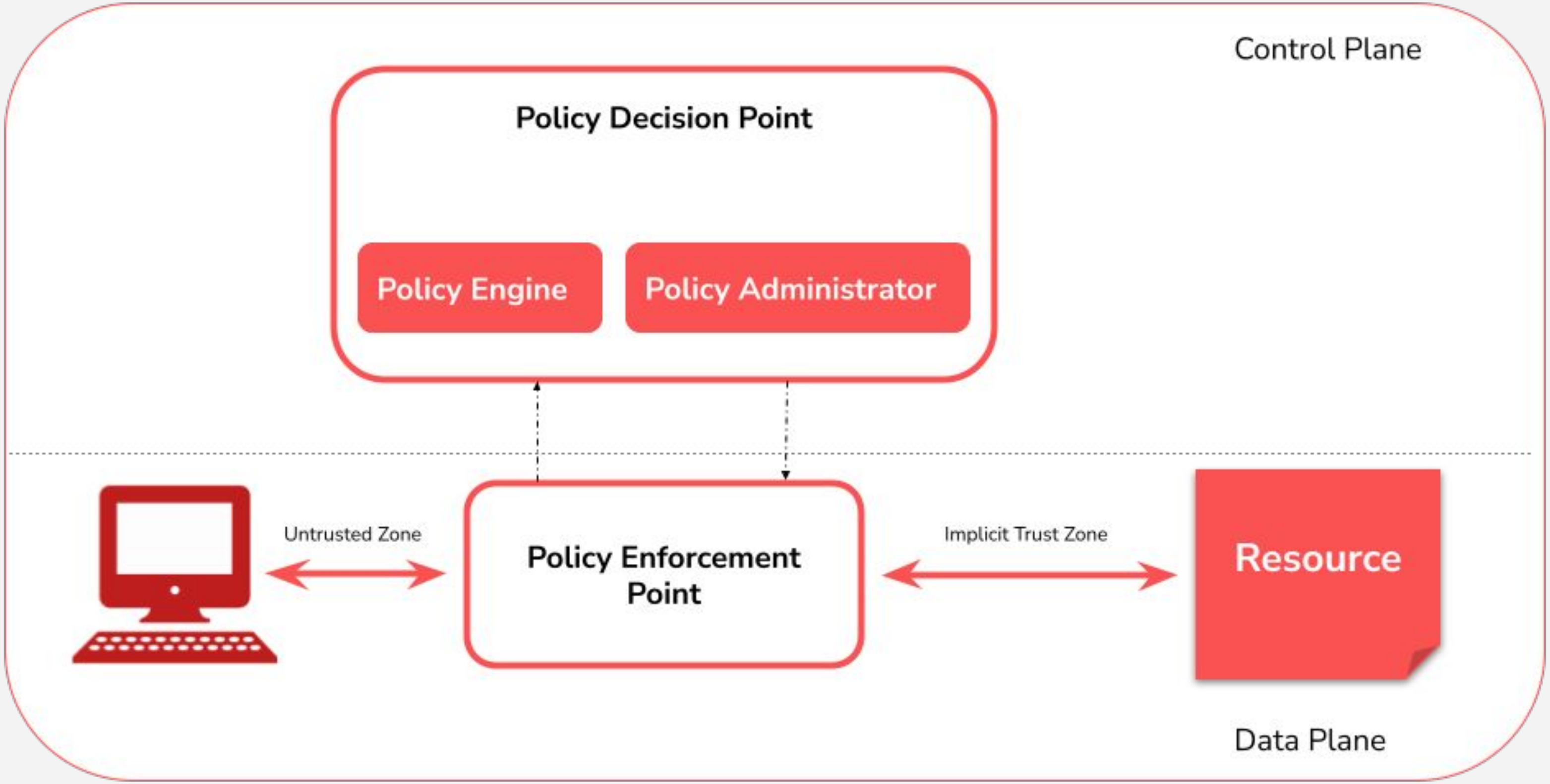
Zero Trust Architecture (ZTA) is split into two logical planes:

Data Plane:

- Contains **Policy Enforcement Point (PEP)**
- Communicates with Policy Decision Point in the Control Plane
- Executes the decisions made by the Control Plane

Control Plane:

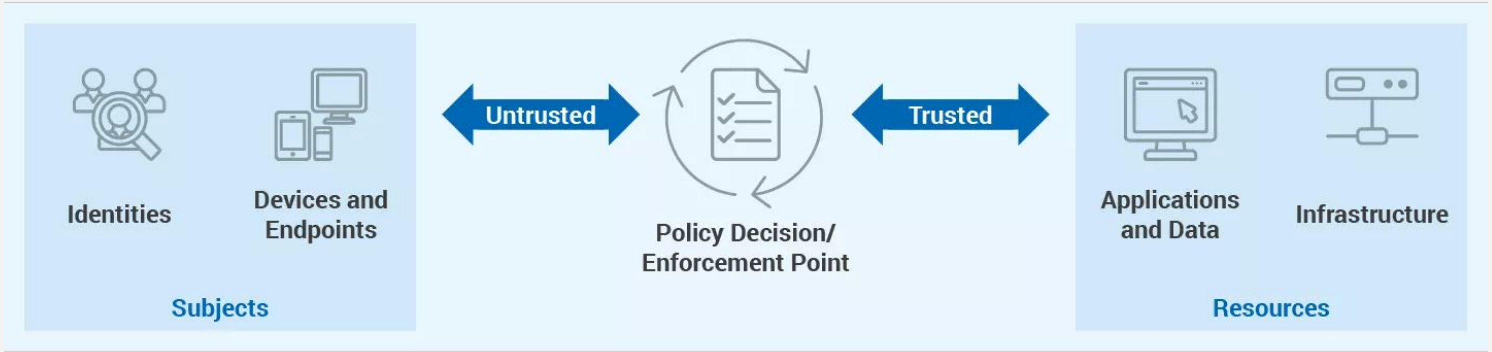
- Provides **attribute-based** access control using the **Policy Decision Point (PDP)**
- Two Parts of the Policy Decision Point:
  - **Policy Administrator:** stores all relevant policies about accessing resources
  - **Policy Engine:** grants or denies access to resources


Control Plane
Policy Decision Point
Policy Engine
Policy Administrator
Untrusted Zone
Policy Enforcement Point
Implicit Trust Zone
Resource
Data Plane

Data Plane

1. User requests to access resource and the **Policy Enforcement Point (PEP)** intercepts request
2. PEP gathers relevant information
    a. **User identity** (e.g., username, role, department)
    b. **Device status** (e.g. health, compliance)
    c. **Location** (e.g., accessing from a trusted network or a public one)
    d. **Time of access** (e.g., working hours or odd hours)
    e. **Sensitivity of the data being accessed**
3. PEP forwards the request and information to the **Policy Decision Point** in the Control Plane.
4. After the PDP makes a decision, the PEP enforces it, granting or denying minimum amount of access necessary to the resource

Zero-Trust Data Plane



Identities

Devices and Endpoints

Subjects

Untrusted

Policy Decision/ Enforcement Point

Trusted

Applications and Data

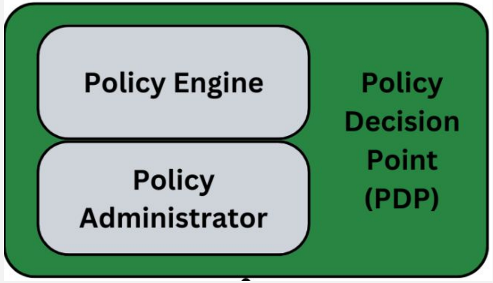
Infrastructure

Resources

Control Plane

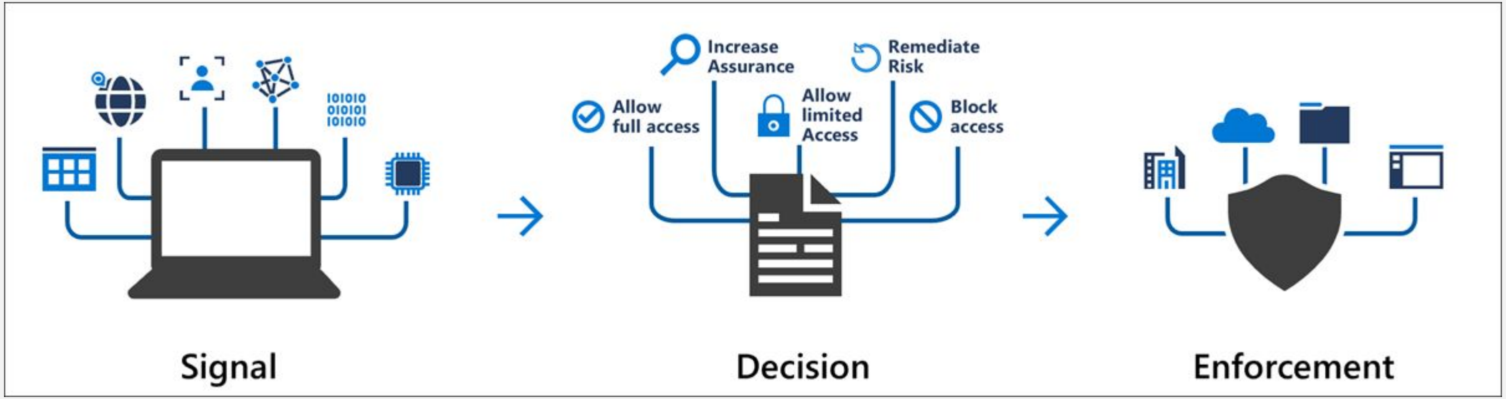
After receiving information from the Policy Enforcement Point:

1. **Policy Engine (PE)** queries the **Policy Administrator (PA)** for applicable access policies:
   a. What kinds of resources does the role have access to?
   b. Can they write to the resource or only read it?
2. **Policy Evaluation and Decision:**
   a. The **PE** evaluates user/device attributes and context against the policies
   b. Policies applies based on the principle of **least privilege** to prevent lateral movement and limit the threat scope
   c. The PE makes an access decision using **adaptive identity**
3. The PDP communicates the decision back to the PEP

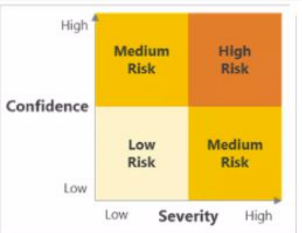


Adaptive Identity

Adaptive Identity: continuously evaluating multiple contextual factors to make real-time access decisions.



Adaptive Identity



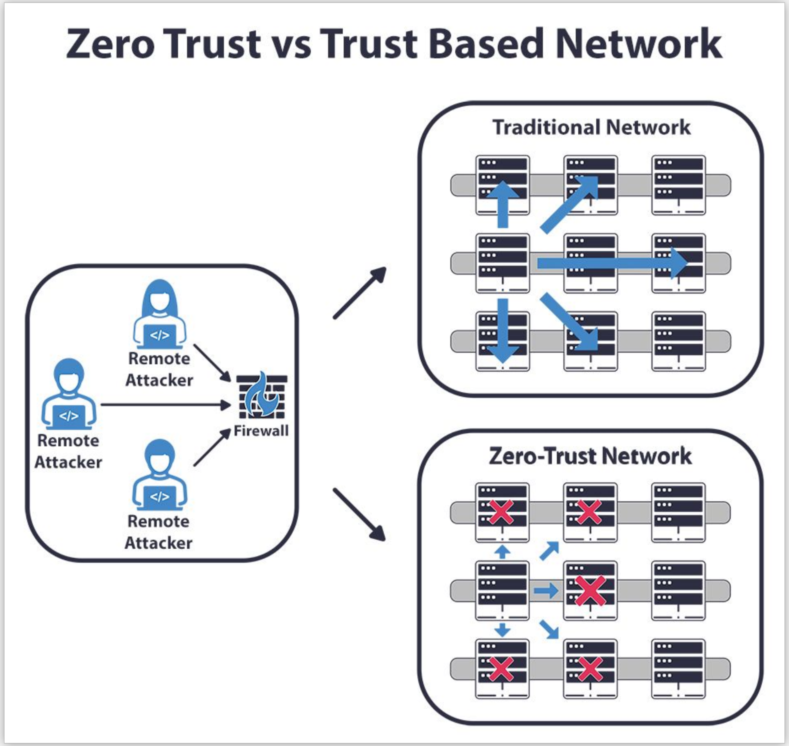
What makes a User/Device **"High-Risk"**?

- Logging in from an unauthorized browser (e.g., TOR)
- Indicators of compromised account (Many failed login attempts, Impossible travel)
- Attempting to access sensitive data from an unusual/highly public location or odd time

Dynamic Decision Making:

- Based on the risk assessment, the PE makes a real-time access decision. This could involve:
  - Granting full access if everything checks out.
  - Granting limited access if some risk factors.
  - Denying access or asking for MFA if high risks are identified.
- The **system adapts its decision based on ongoing monitoring** and changing conditions. If new information comes in or if the context changes, the access permissions are adjusted accordingly.

Preventing Lateral Movement



Example:

1. **User Request:** You request access to a financial report.
2. **PEP Interception:** The Policy Enforcement Point **(PEP) intercepts** your request and sends it to the Policy Decision Point (PDP).
3. **Request Evaluation:** The **PDP retrieves relevant policies** from the Policy Administrator and the Policy Engine evaluates your request based on your role, the resource, and context of the request.
4. **Adaptive identity Check:** The **Policy Engine applies security controls** based on various factors in real-time such as:
   a. Device configuration
   b. User behavior
   c. Location/Time of Day
   d. IP Address
5. **Decision Communication:** The **PE decides how much access** to give you and the PDP communicates the PE's decision to the PEP.
6. **PEP Enforcement:** The **PEP enforces the decision**, granting or denying access to the financial report.
7. **Continuous Monitoring:** The **PEP regularly checks with the PDP** to ensure that any changes in your access rights are immediately updated.