# Zero Trust

Zero Trust Model en Architectuur

## Intel Project Amber to Launch in Mid-2023

On top of Intel TDX, the company also plans to launch Project Amber in mid-2023. Intel first introduced the project last year, which is designed to create a new multi-cloud, multi-TEE service for third-party attestation, aligning with zero-trust principles.

[redacted]

MIT News
ON CAMPUS AND AROUND THE WORLD

SUBSCRIBE

## Zero-trust architecture may hold the answer to cybersecurity insider threats

MIT Lincoln Laboratory study explores a new approach to securing systems.

HOME

# Make 2023 the year of zero trust

10 January 2023

Articles / News

## U.S. Government Bolsters Zero-Trust Adoption in 2022

Nancy Liu | Editor
December 30, 2022 6:00 PM

Share this article:

# Wat is Zero Trust

- Zero Trust is een security model, strategie en een framework dat niets vertrouwt.
  - ✓ Vertrouw nooit, maar verifieer
  - ✓ Gaat uit van een hack
  - ✓ Verifieer expliciet
  - ✓ Minimale toegang
- Minimale Uitgangspunten
  - Gaat uit van een vijandig netwerk
  - Externe en interne dreigingen zijn er altijd
  - Locatie is niet genoeg om vertrouwen vast te stellen
  - Elke gebruiker, apparaat en netwerk stroom wordt met dynamische policies geauthentiseerd en geautoriseerd.

- **Zero Trust is een strategie en framework vergelijkbaar met ITIL voor SM en Agile voor PM**

# Zero Trust definities


- Zero Trust is een strategie op hoog niveau die ervan uitgaat dat personen, apparaten en diensten die proberen toegang te krijgen tot bedrijfsbronnen, zelfs degenen binnen het netwerk, niet automatisch kunnen worden vertrouwd. Om de veiligheid te vergroten worden deze gebruikers elke keer dat ze toegang vragen, geverifieerd, zelfs als ze al eerder zijn geverifieerd.
- Zero Trust is een beveiligingsmodel, een reeks systeemontwerpprincipes en een gecoördineerde cyberbeveiligings en systeem managementstrategie waarbij bedreigingen zowel binnen als buiten het traditionele netwerk bestaan.
-

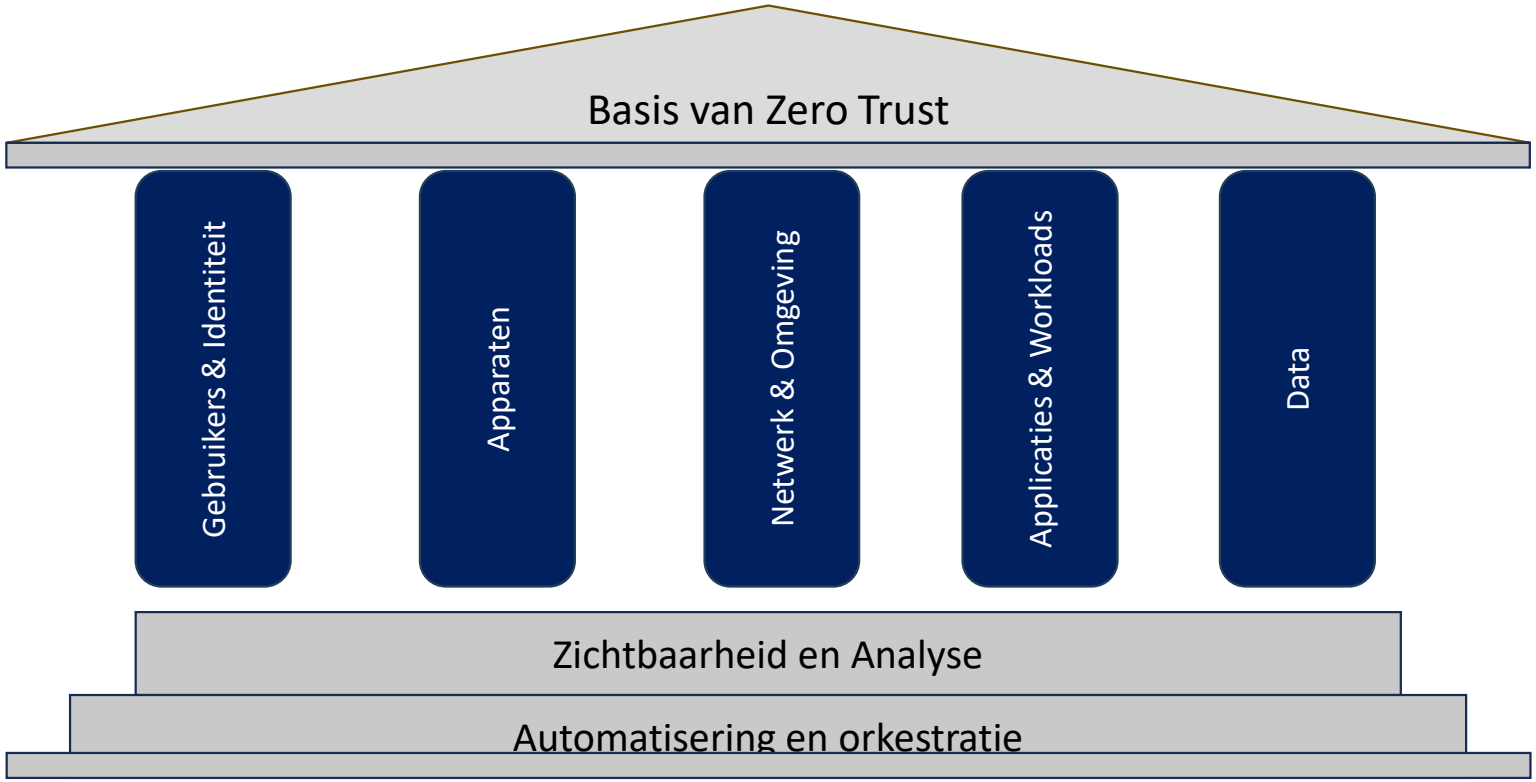
# Never Trust, Always Verify

- Vertrouwen is Niet impliciet
- Vertrouwen is een kwetsbaarheid
- Elk apparaat, verzoek en elke gebruiker is een dreiging tot positief geverifieerd.
- Gebruikt Just-in-Time en Just-enough-Access minimale toegangs controles

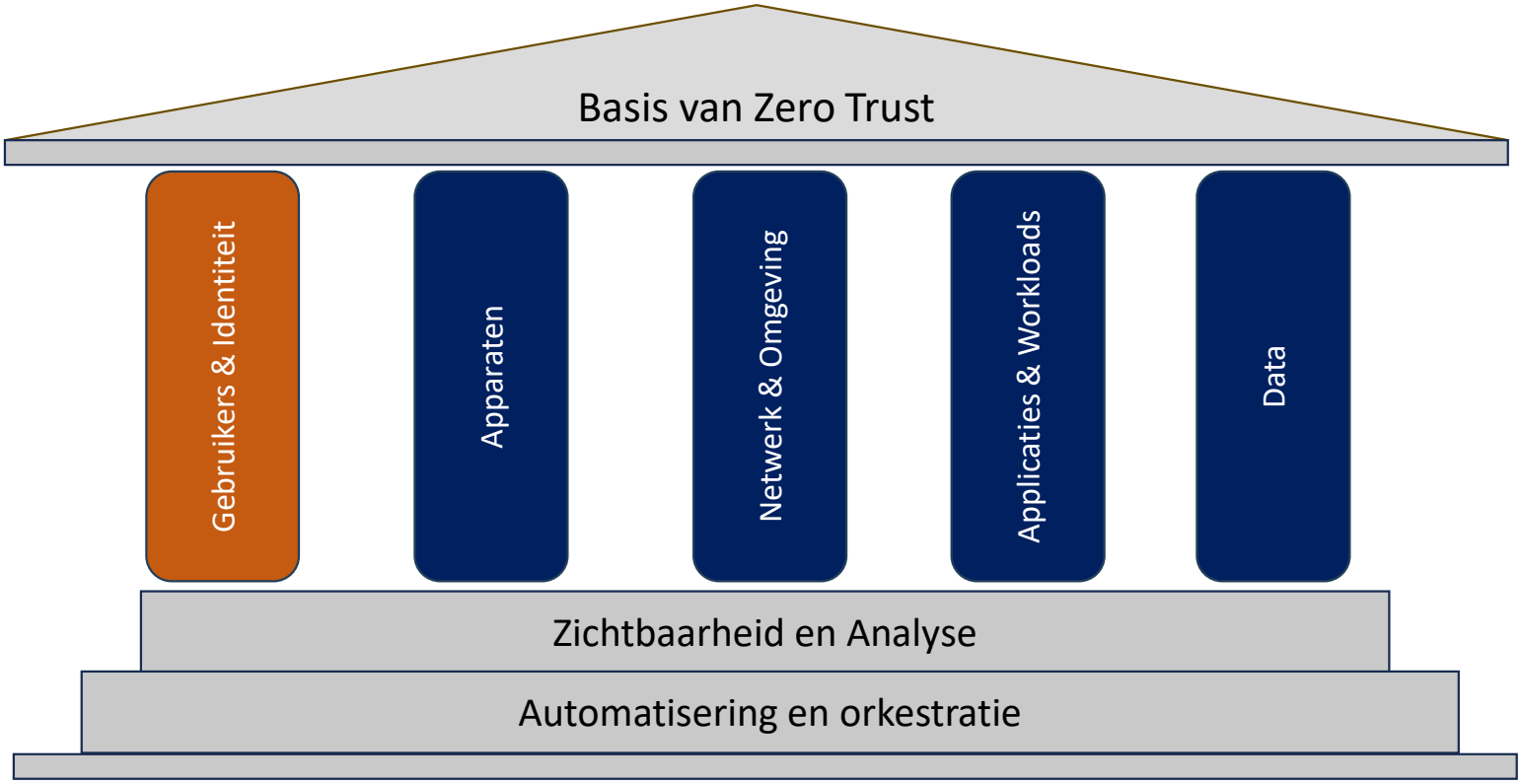
# Zero Trust Principes

- Elke data bron en elke computer is een resource
- Alle communicatie is beveiligd onafhankelijk van locatie
- Toegang wordt verleent per sessie, JIT/JEA
- Beperk toegang met een dynamische policy
- Manage Data integriteit
- Dwing authenticatie en autorisatie af
- Verzamel data voor verbeterde security

# Zero Trust Pilaren

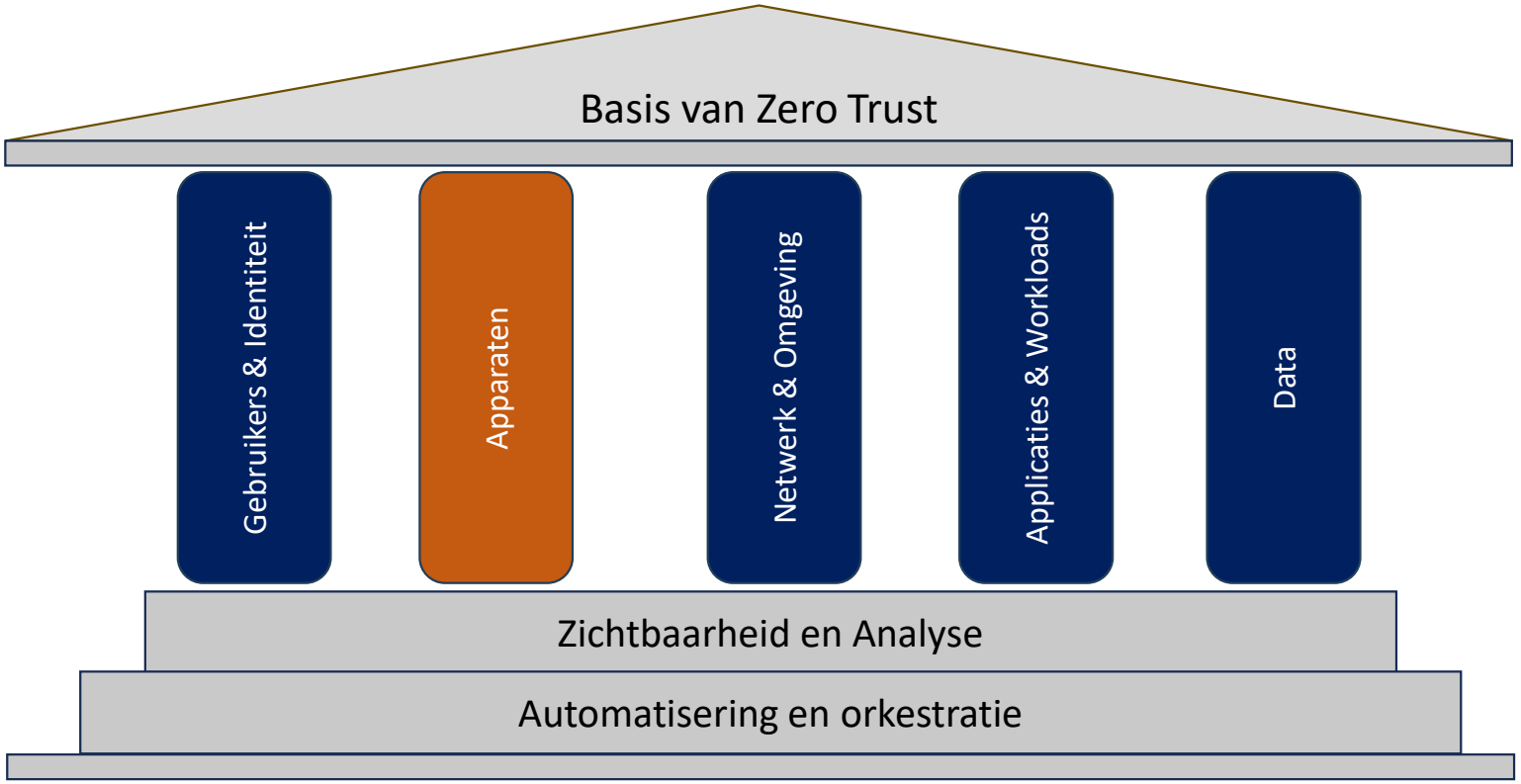


# Zero Trust Pilaren



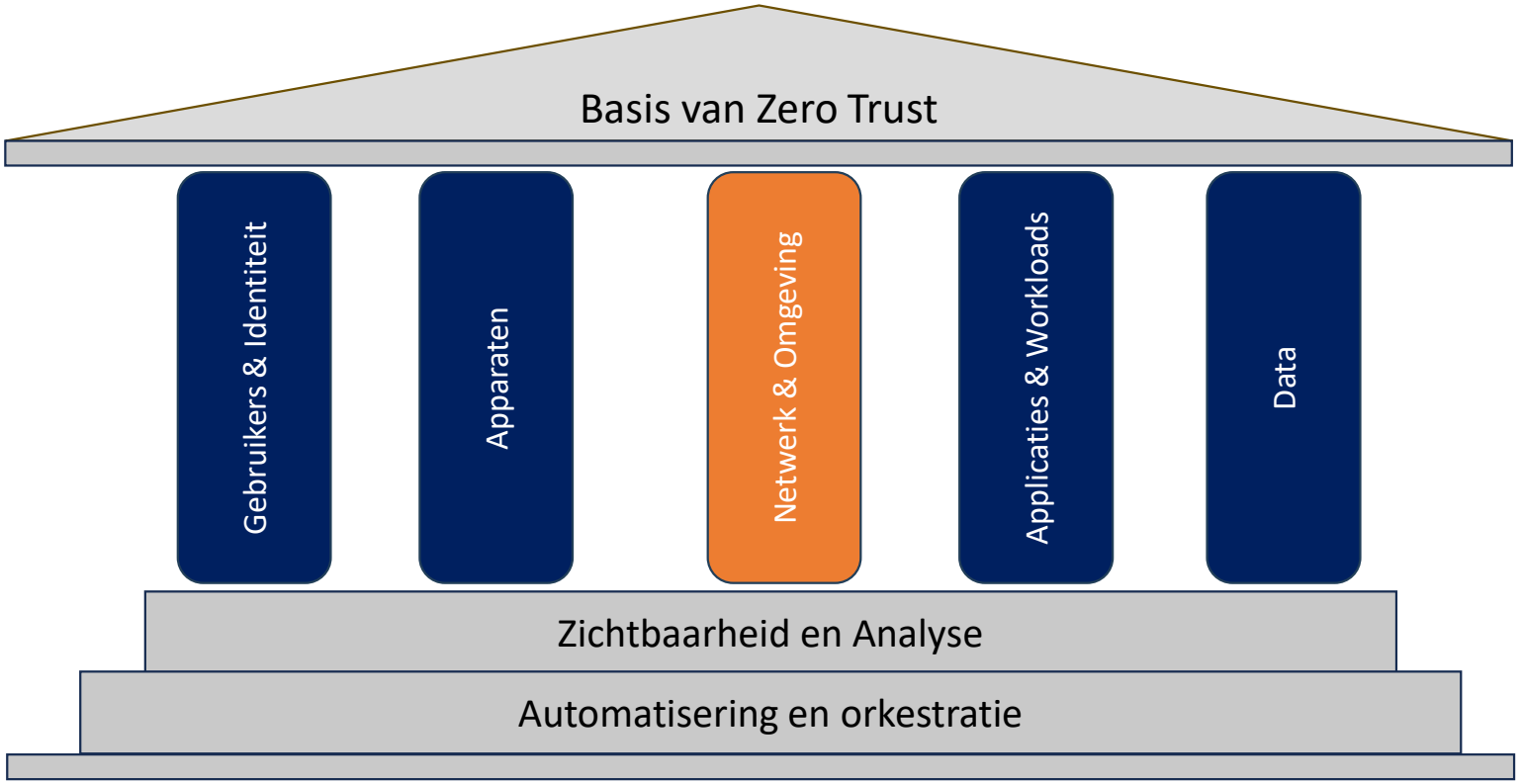

Gebruiker identificatie, authenticatie en toegangscontroles met behulp van dynamische en contextuele data-analyse

# Zero Trust Pilaren



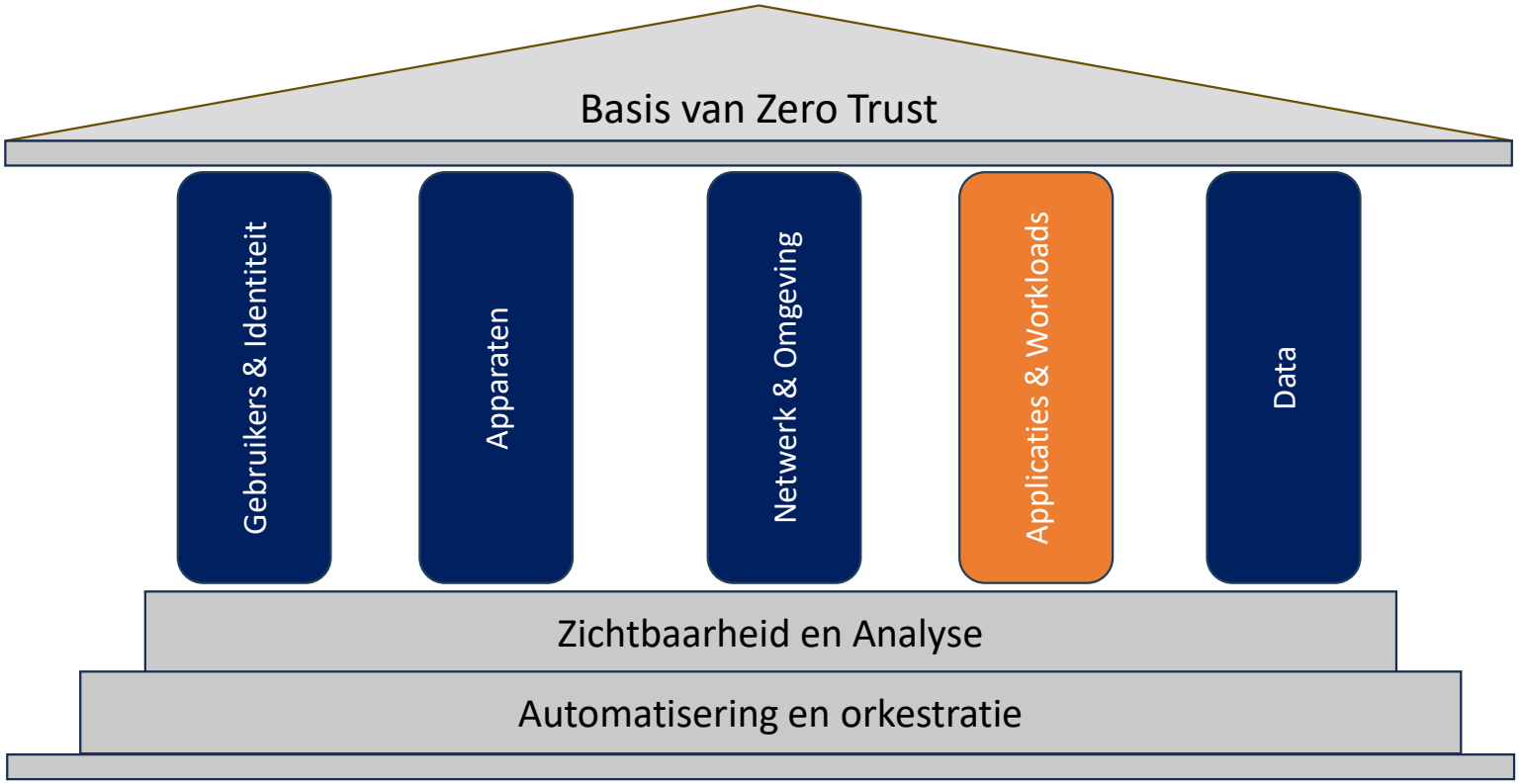

Valideer of apparaten voldoen aan gedefinieerde standaarden en normen.

# Zero Trust Pilaren



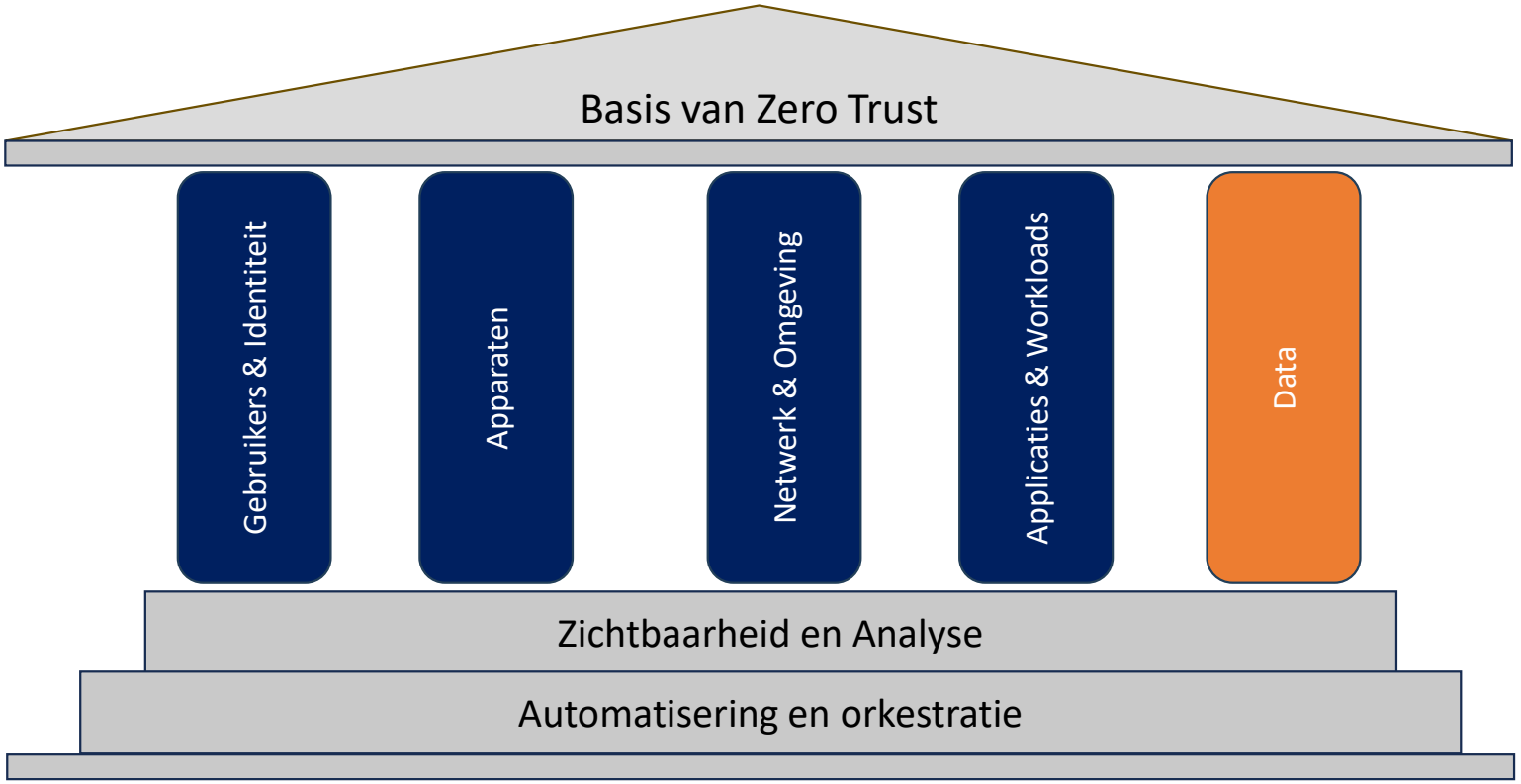

Segmenteer isoleer en controleer het netwerk met specifieke policies en toegangscontroles

# Zero Trust Pilaren



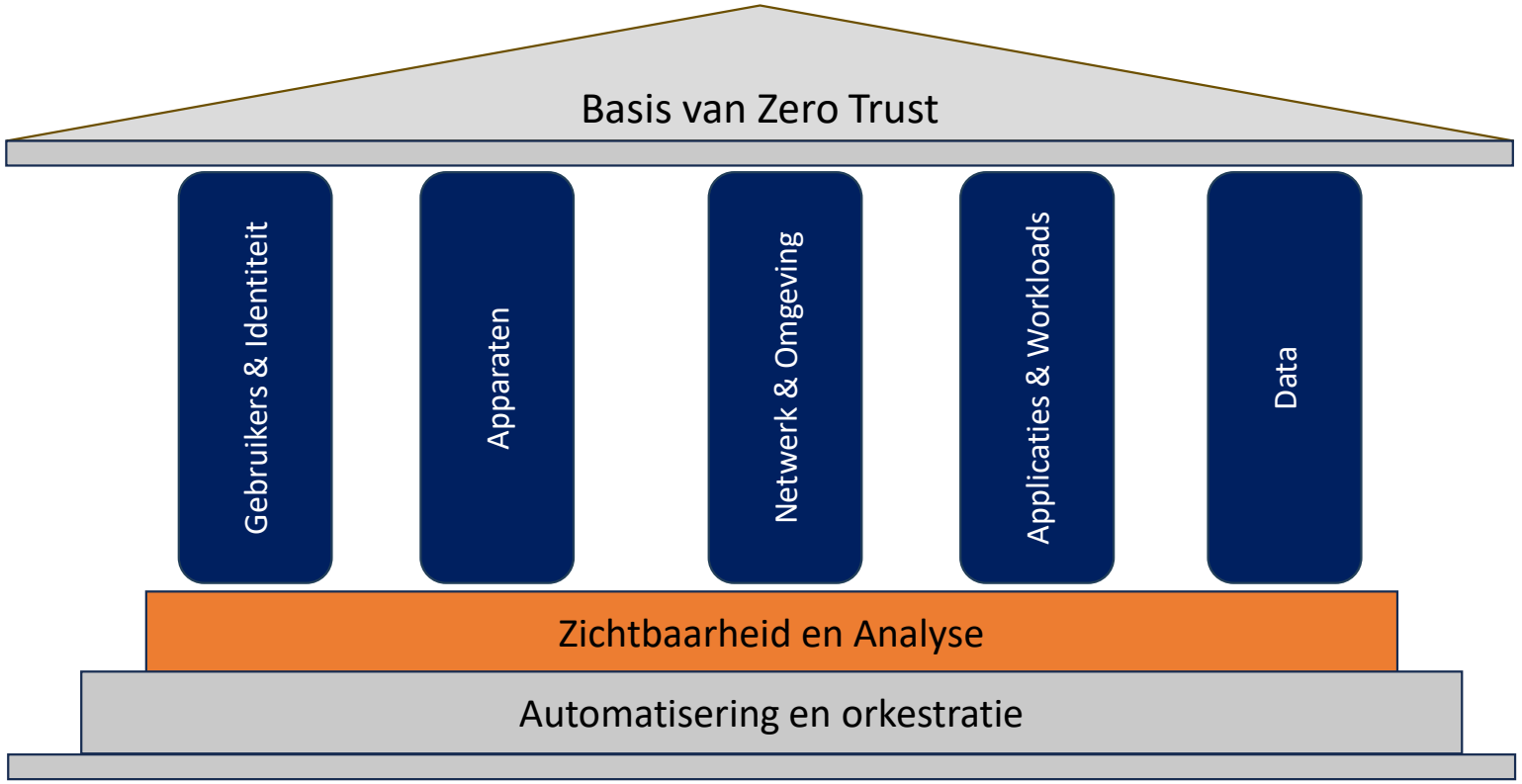

beveilig alles van applicaties tot hypervisors, inclusief containers en virtuele machines.

# Zero Trust Pilaren



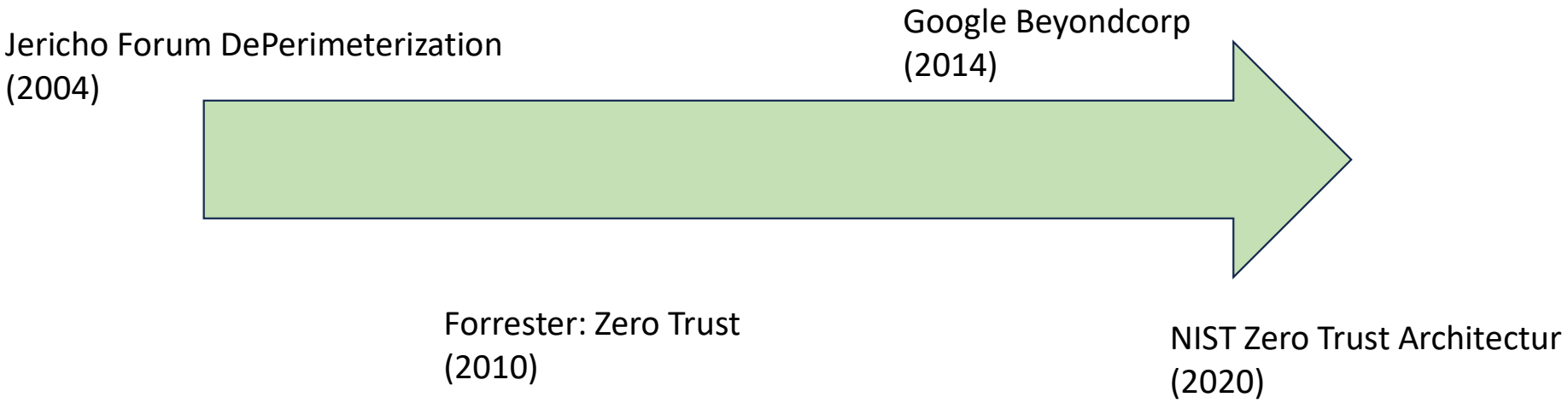

toegangsbeveiliging op basis van het categoriseren van gegevensclassificatie

# Zero Trust Pilaren

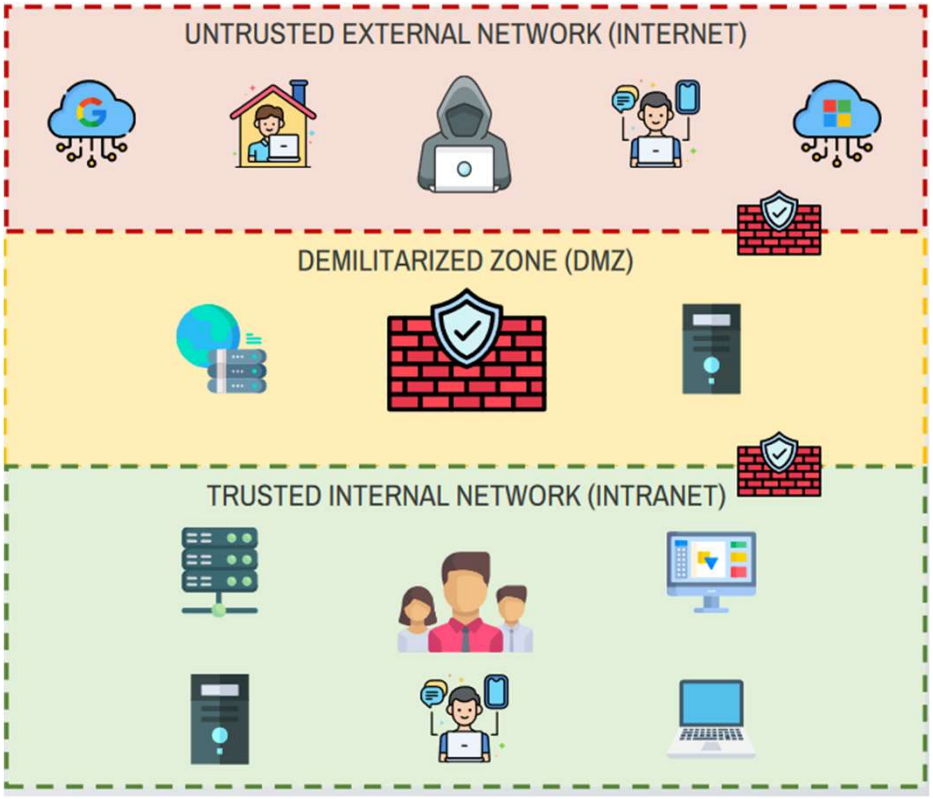



Inzicht in gedrag van gebruikers en systemen door real-time monitoring

# Zero Trust is niet nieuw.



# Waarom Zero Trust

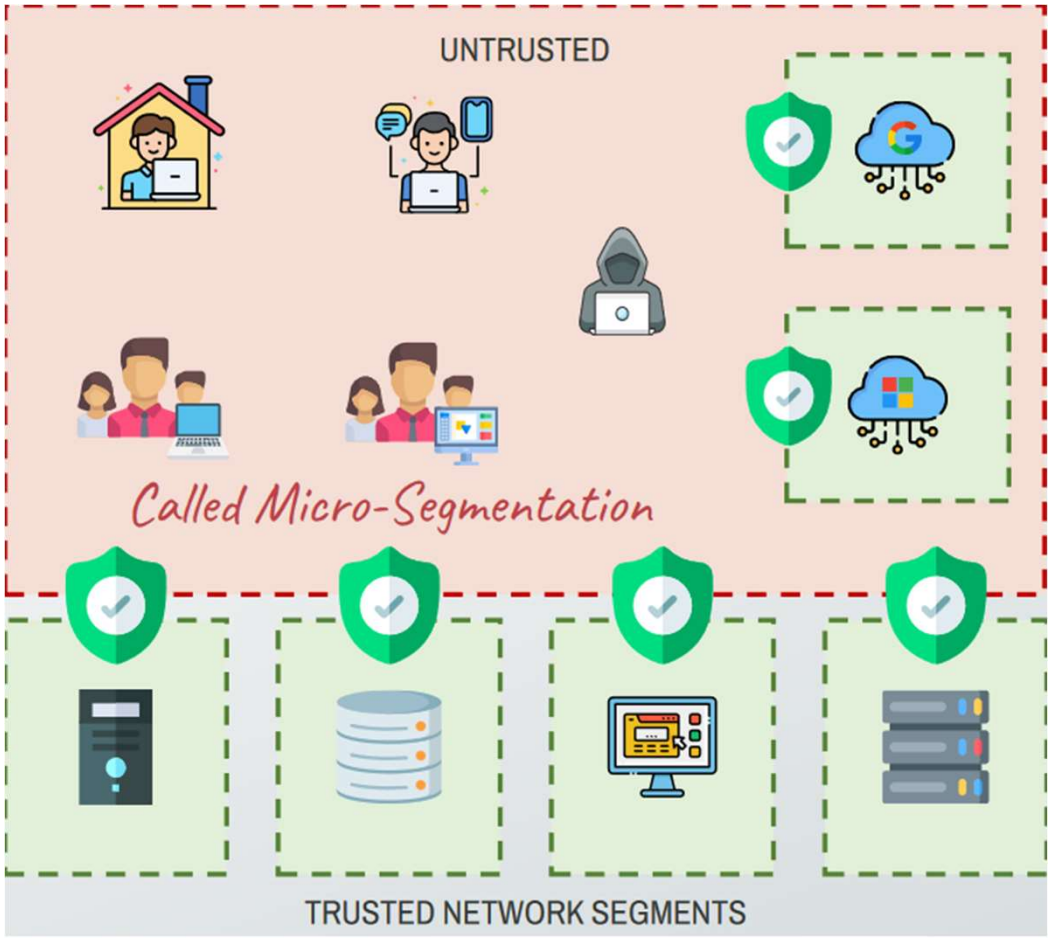



## Evolutie van IT

- ✓ IT begon met een betrouwbaar en niet betrouwbaar netwerk
- ✓ DMZ voor Internet facing diensten
- ✓ Thuiswerken en BYOD werd normaal
- ✓ Cloud diensten werden vaak de norm

Hiermee loste de grens tussen betrouwbaar en onbetrouwbaar op.

# Zero Trust Architectuur




- Gebruikers en apparaten zijn onbetrouwbaar
- Vertrouwd netwerk opgeknipt in segmenten
  - Beperkt inbreuk zones en voorkomt zijdelingse beweging door hackers
- Cloud diensten zijn gesegmenteerd
- Segmenten worden beschermd door intelligente "policy decision points"

# Valkuilen grensbewaking

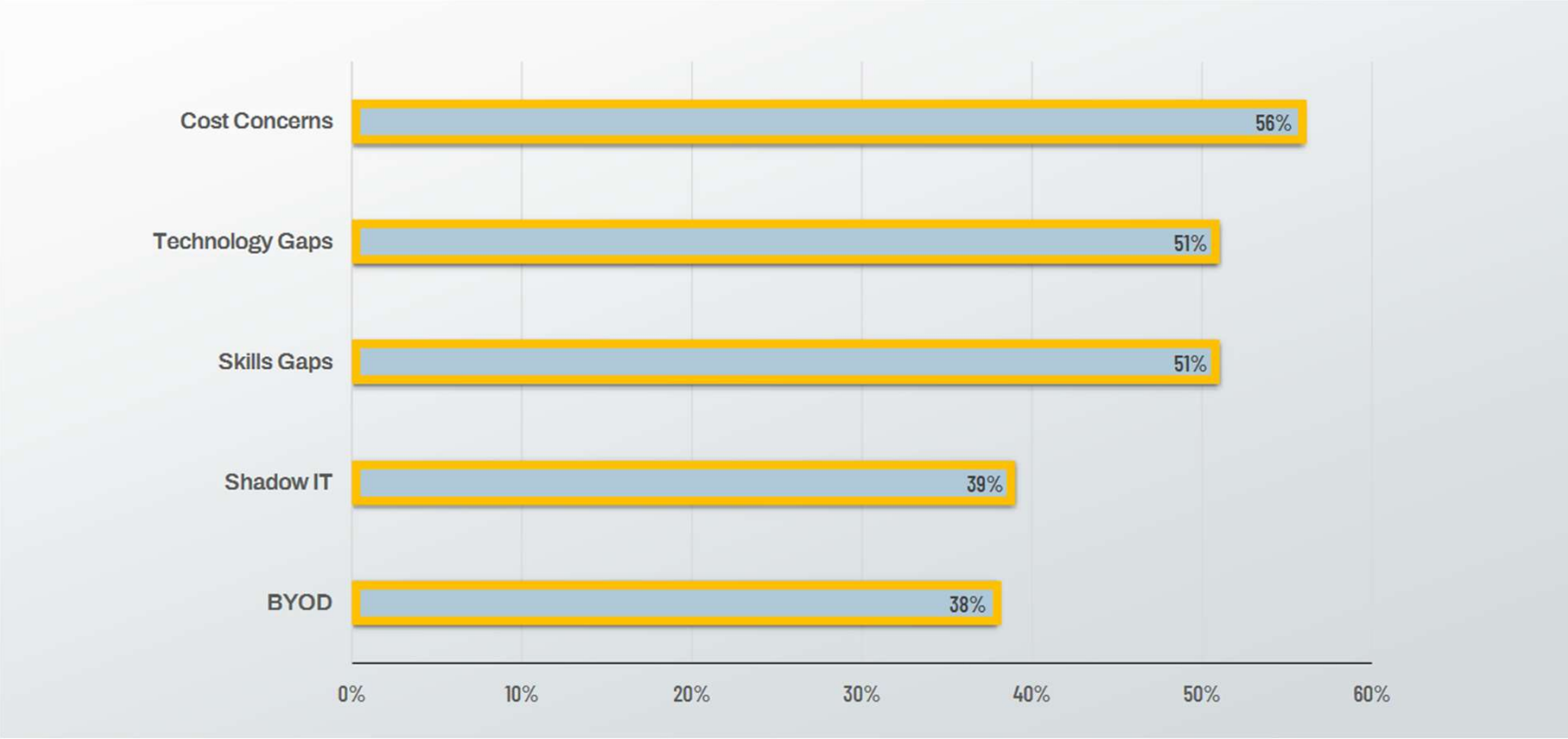
- Mindset
- Perimeter mindset, buiten vs binnen
- Vertouwen door te controleren
- Statische policies
- Dreiging van binnenuit
- Zijwaardse beweging

# Zero Trust voordelen Gartner

- 75% rapporteerde verbeterd risico management
- 65% rapporteerde verbeteringen in beveiligde toegang op afstand
- 41% rapporteerde minder IT security incidenten
- 34% rapporteerde verminderde netwerk complexiteit
- 26% rapporteerde lagere overall security kosten

- Gartner Peer Insights & WatchGuard: Zero Trust Security Strategy Adoption Survey (2021)

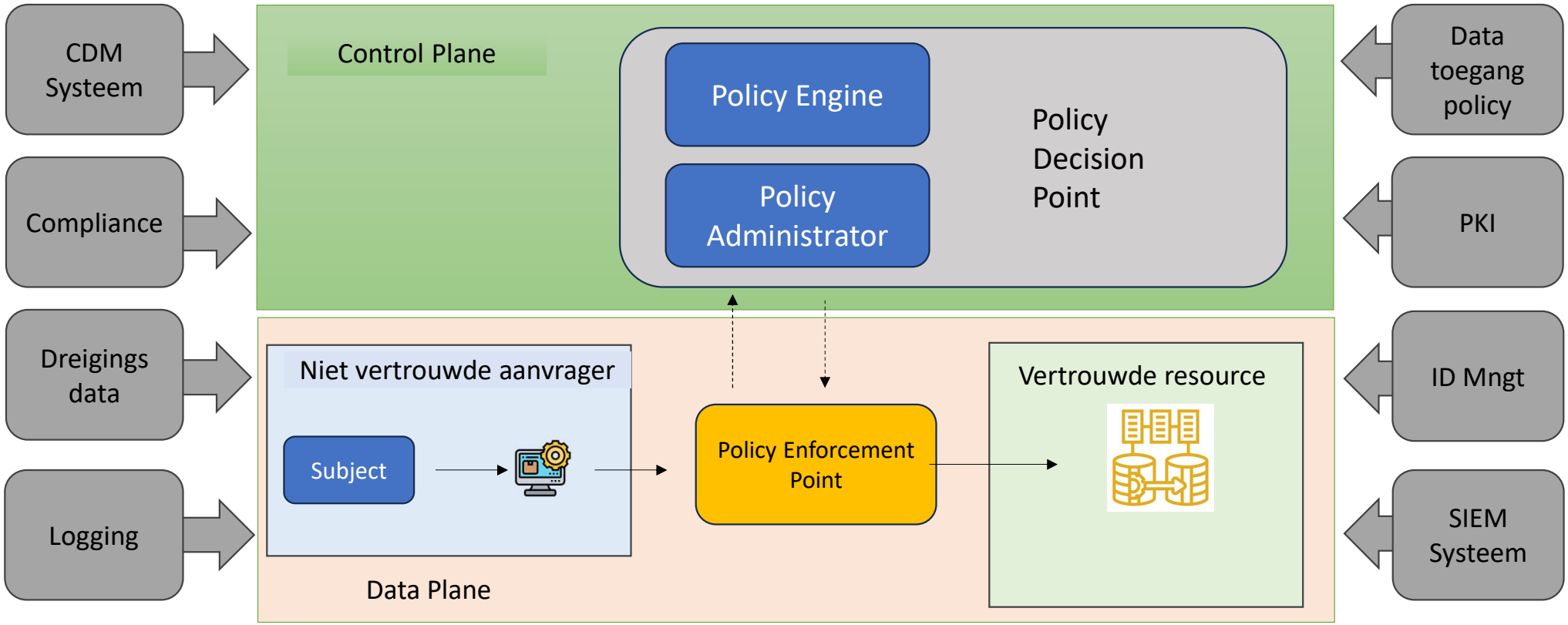
# Zero Trust adoptie zorgen




Zero Trust Architectuur

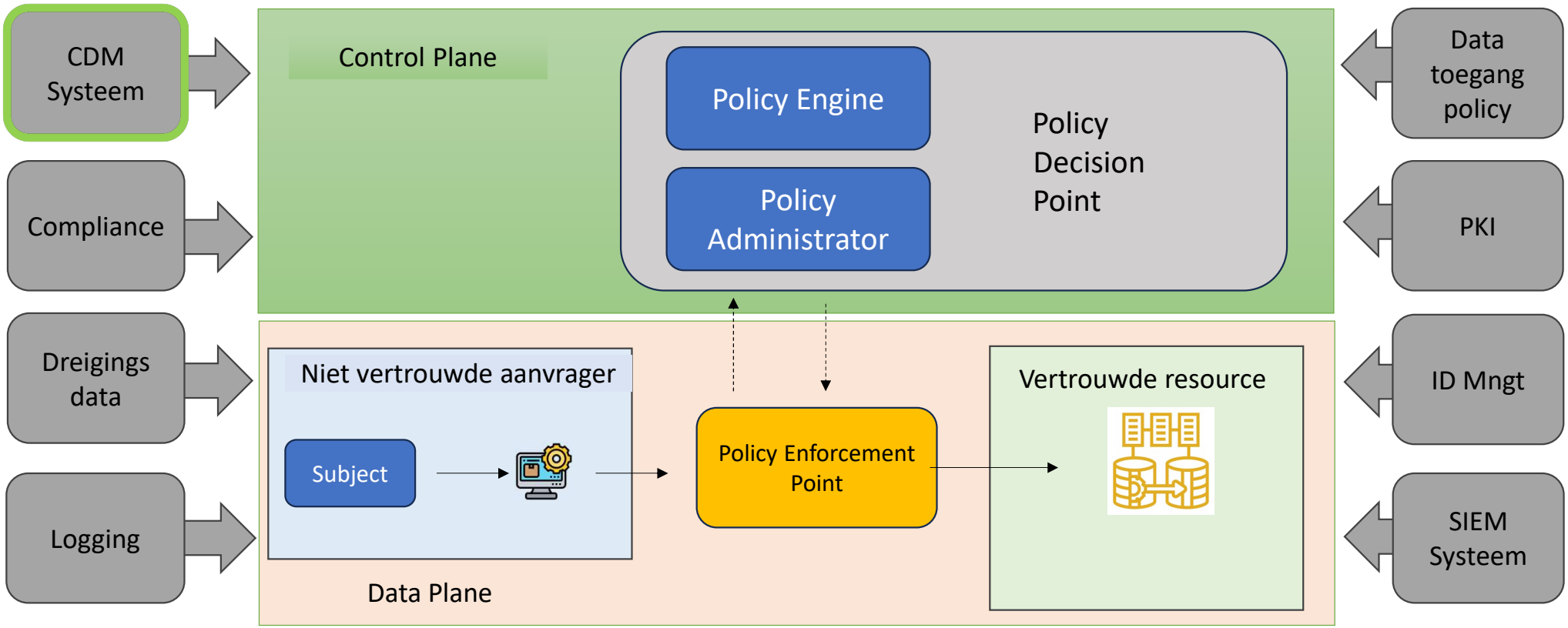
# NIST Zero Trust Architectuur Model

Breed geaccepteerd onafhankelijk conceptueel model



# NIST Zero Trust Architectuur Model

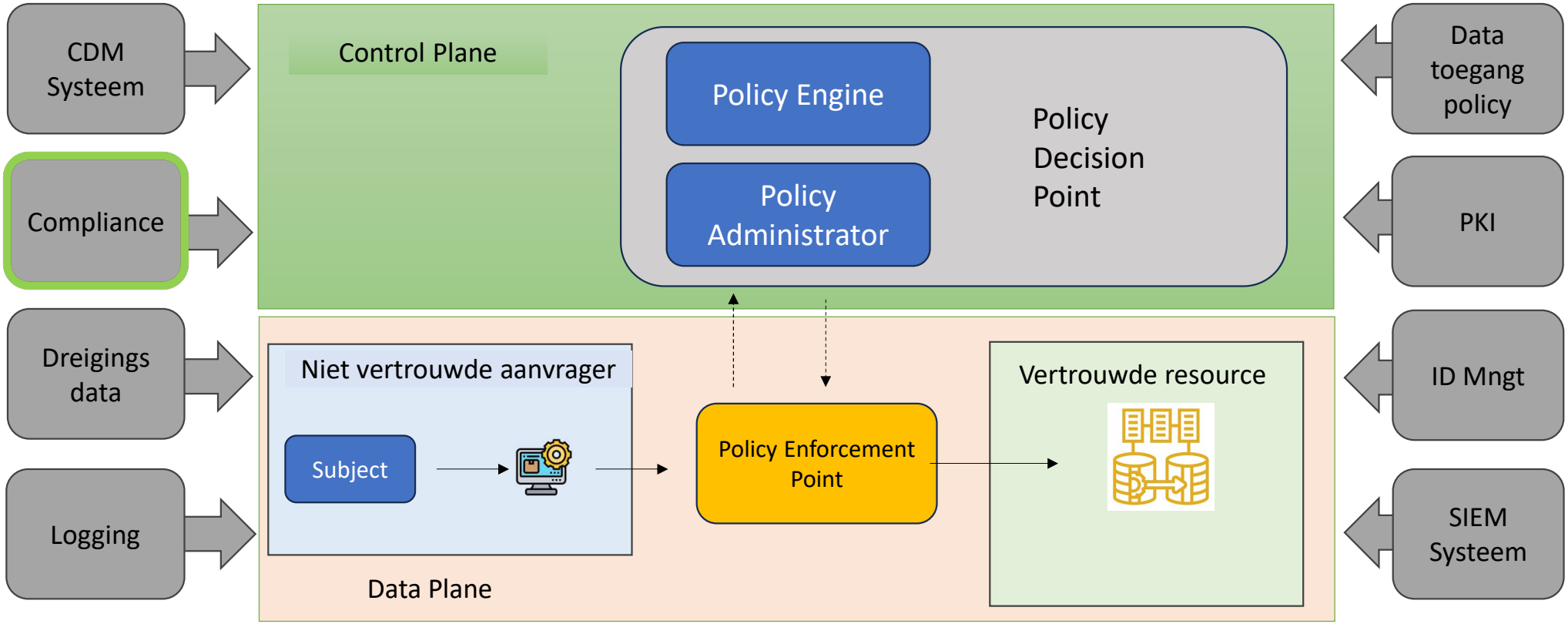
ZTA Data bronnen




Continuous Diagnostics en Mitigation; verzamelt informatie mbt bedrijfssystemen en bepaalt hun huidige staat en zorgt voor configuratie en software updates waar van toepassing

# NIST Zero Trust Architectuur Model

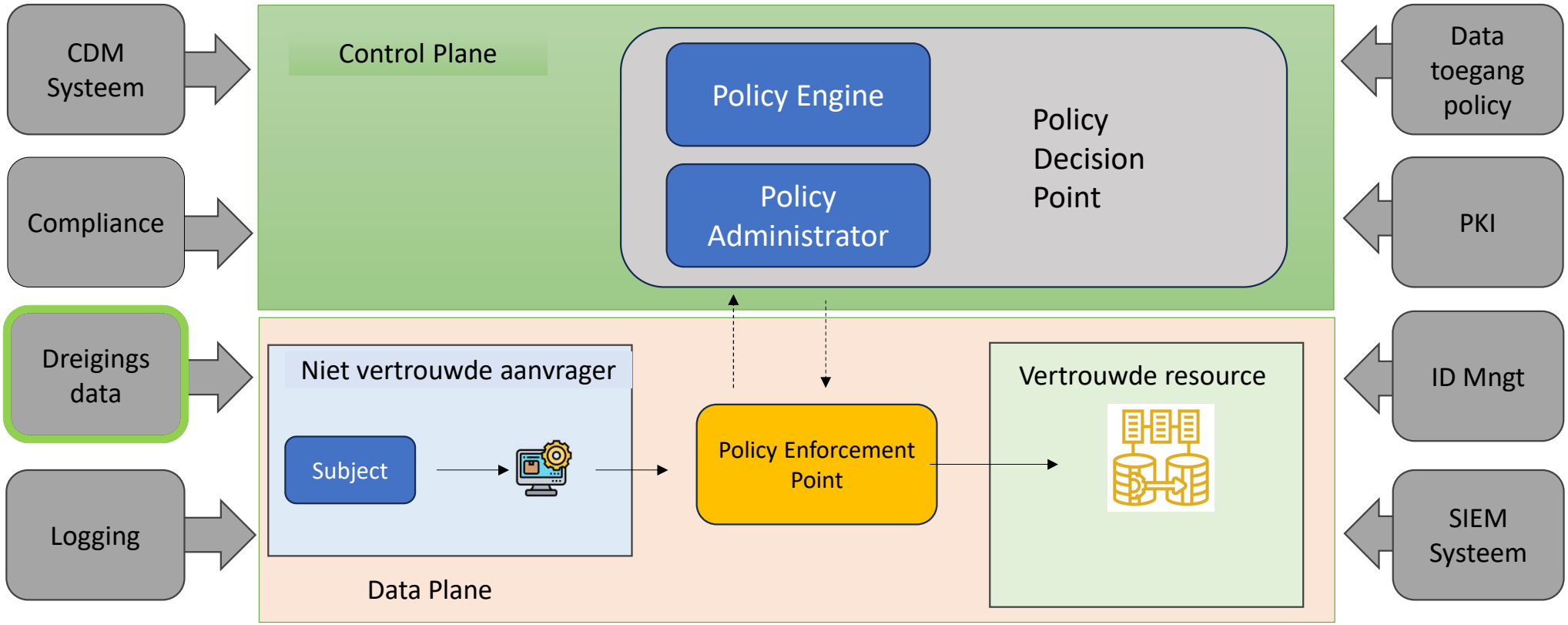
ZTA Data bronnen




Dit systeem zorgt ervoor dat de onderneming blijft voldoen aan de wettelijke vereisten zsoals ISO27001, FISMA, BIO, NEN7510

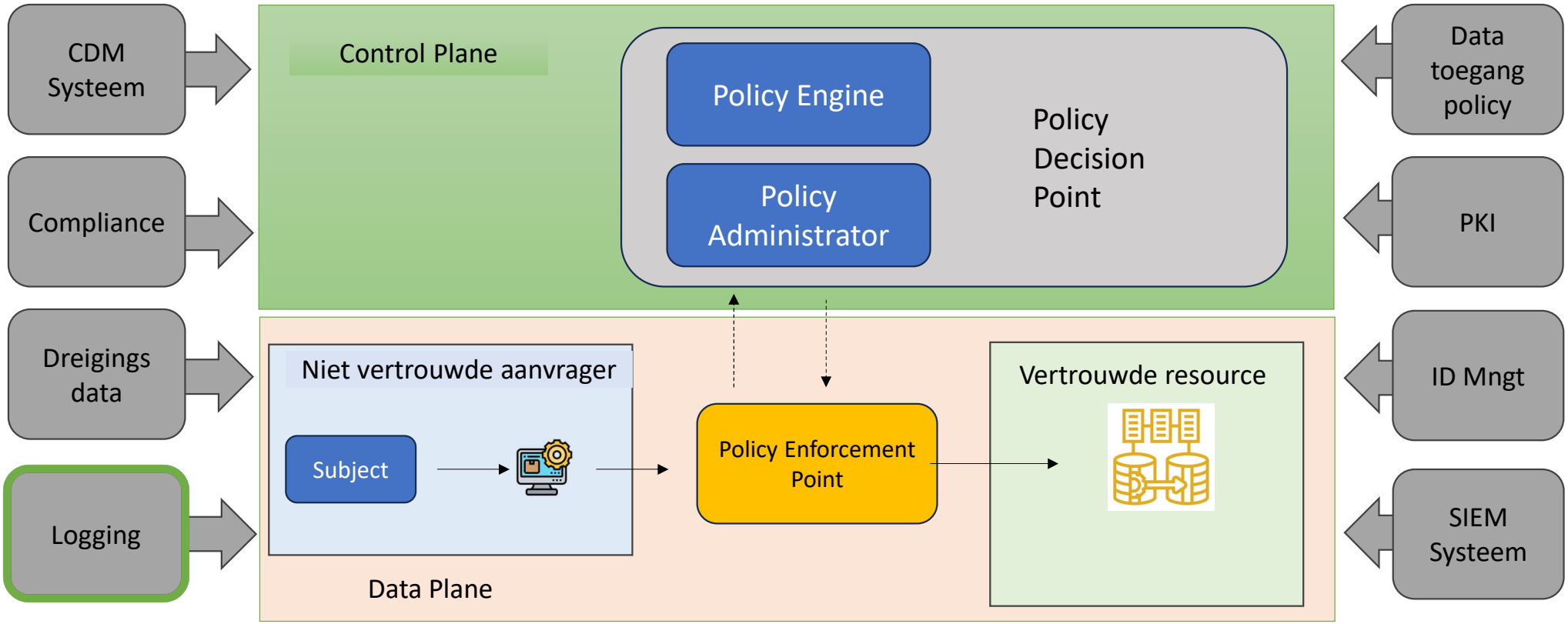
# NIST Zero Trust Architectuur Model

ZTA Data bronnen



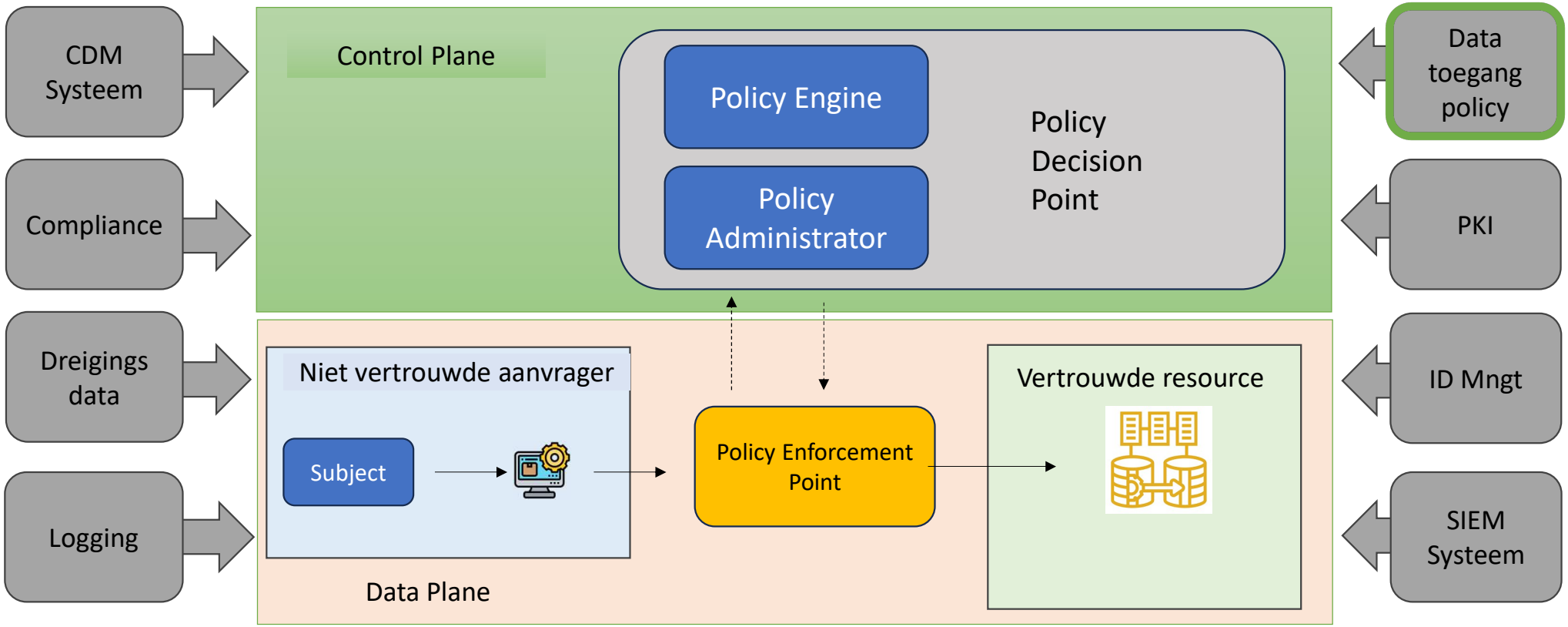
# NIST Zero Trust Architectuur Model

ZTA Data bronnen



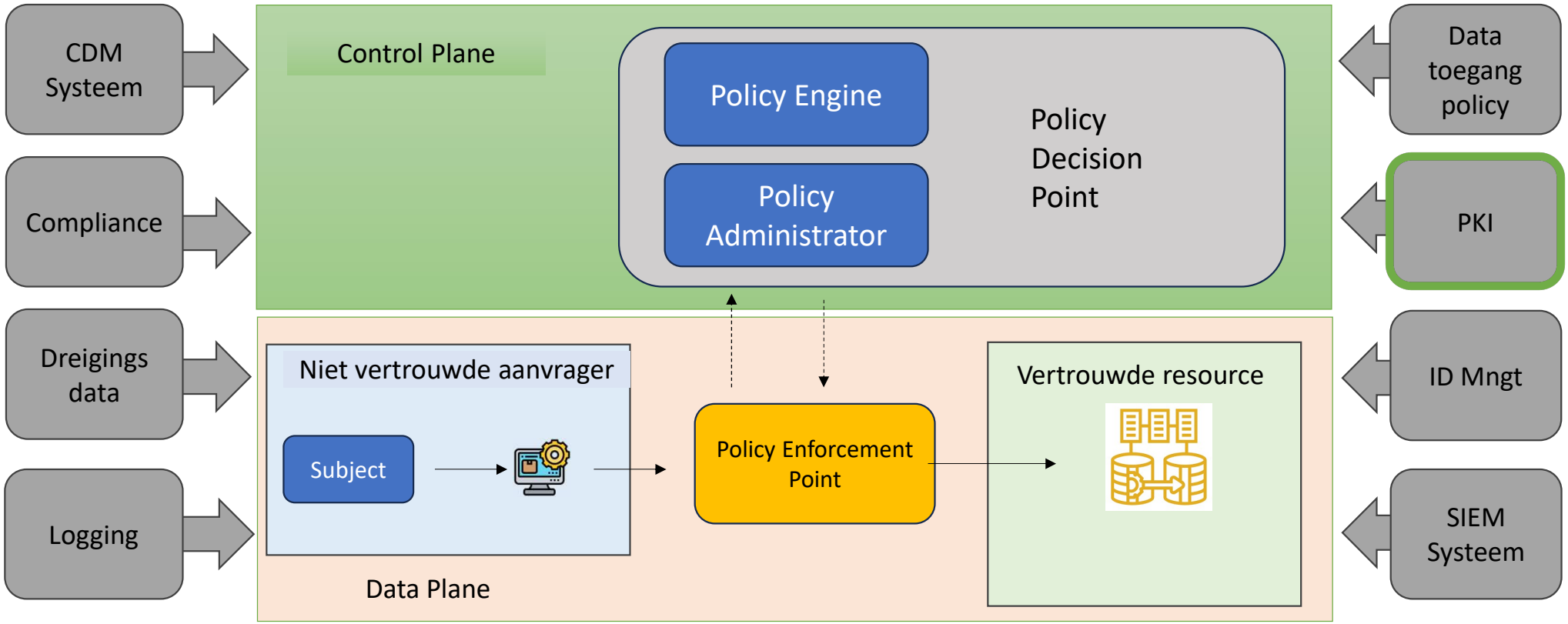
# NIST Zero Trust Architectuur Model

ZTA Data bronnen



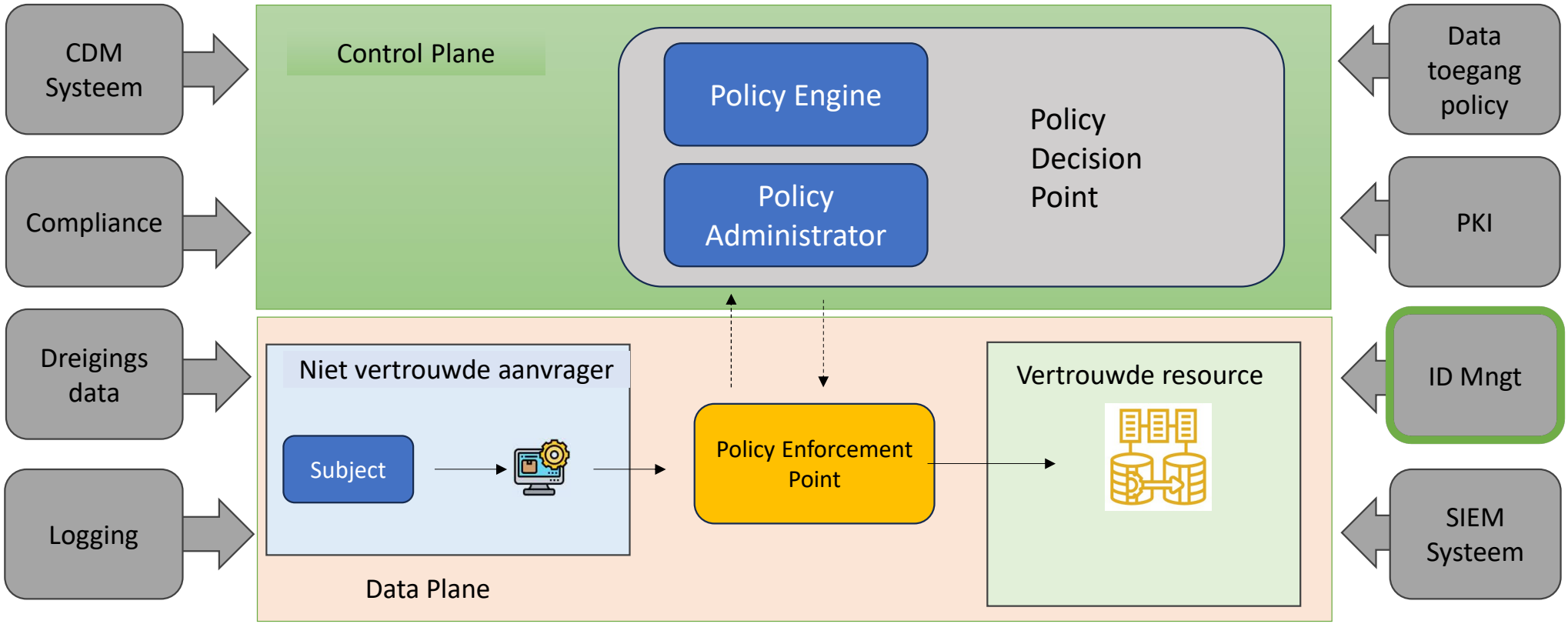
# NIST Zero Trust Architectuur Model

ZTA Data bronnen



# NIST Zero Trust Architectuur Model

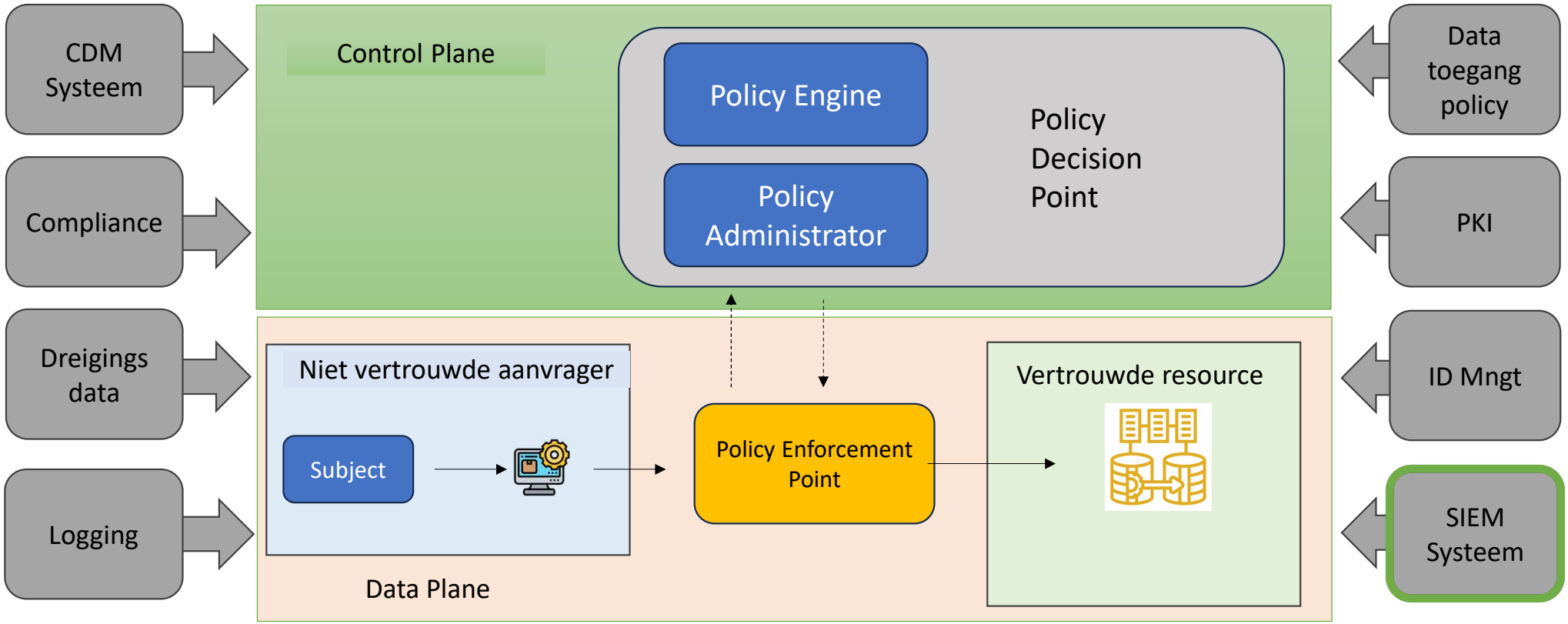
ZTA Data bronnen




ID-beheersysteem: Dit systeem is verantwoordelijk voor het aanmaken, opslaan en beheren van zakelijke gebruikersaccounts en identiteitsregistraties

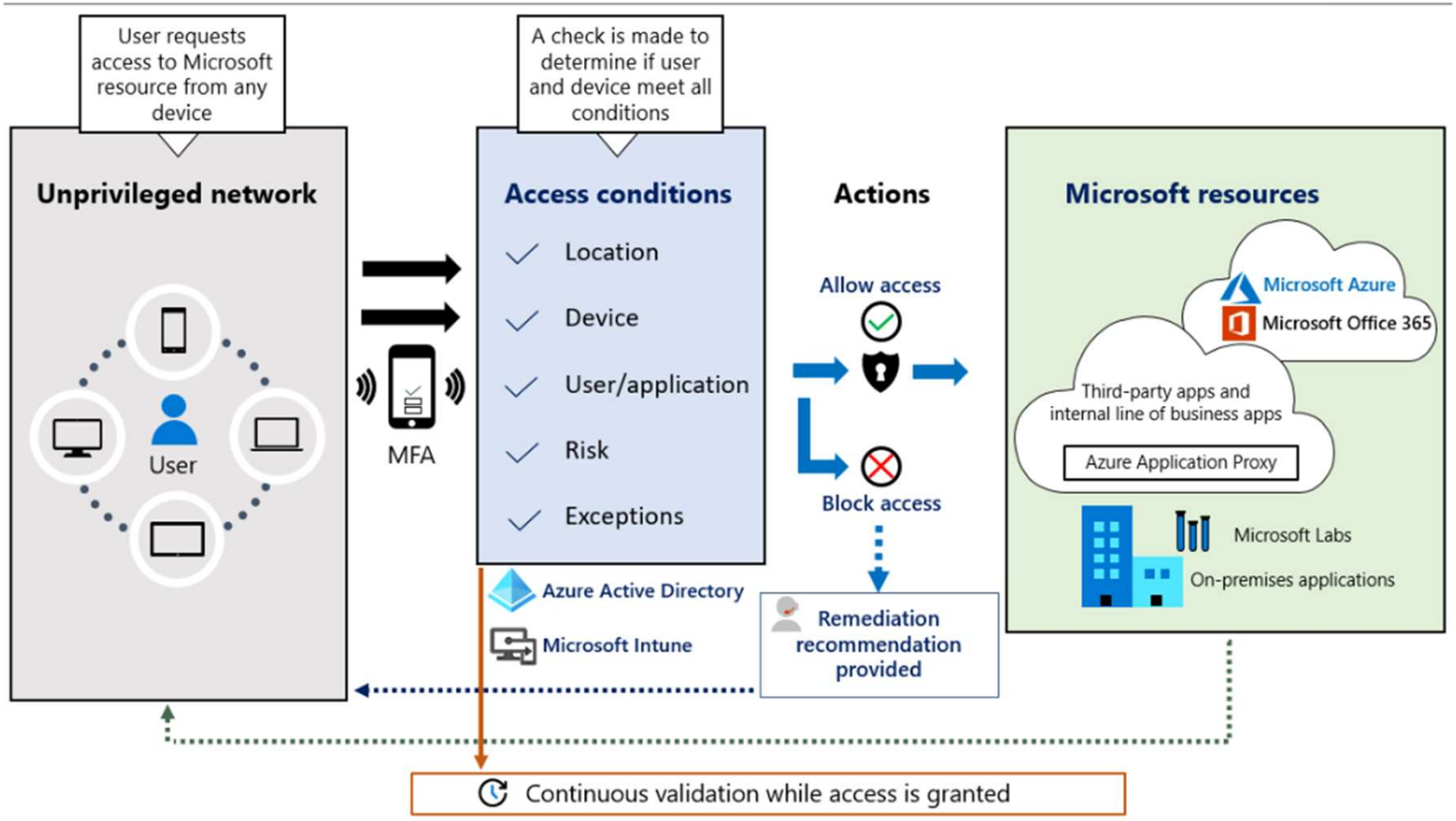
# NIST Zero Trust Architectuur Model

ZTA Data bronnen



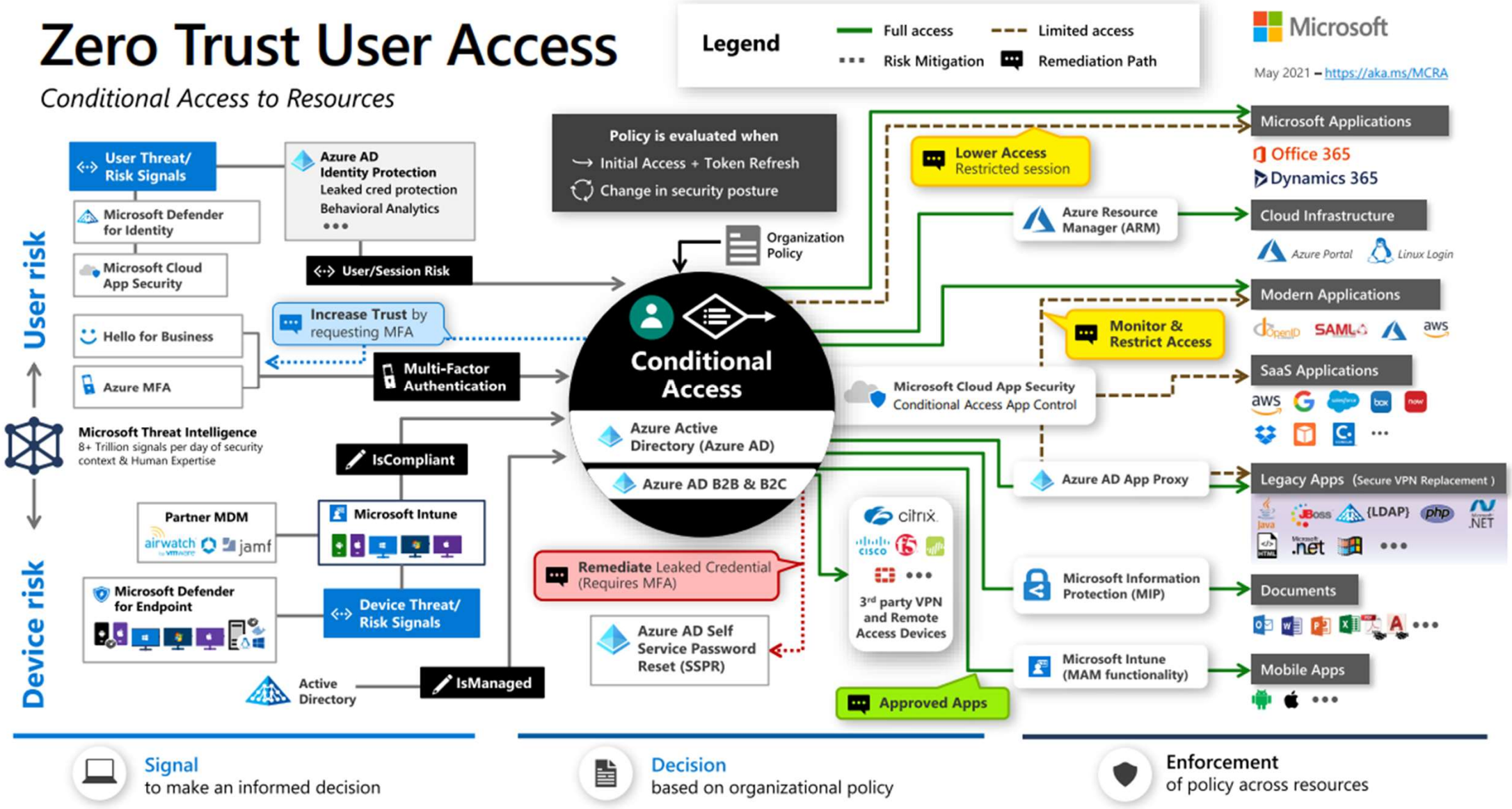

Het SIEM-systeem verzamelt, aggregeert en analyseert op beveiliging gerichte informatie, die de organisatie helpt potentiële cyberdreigingen te herkennen en beleid te verfijnen

# Microsoft's interne ZTA oplossing

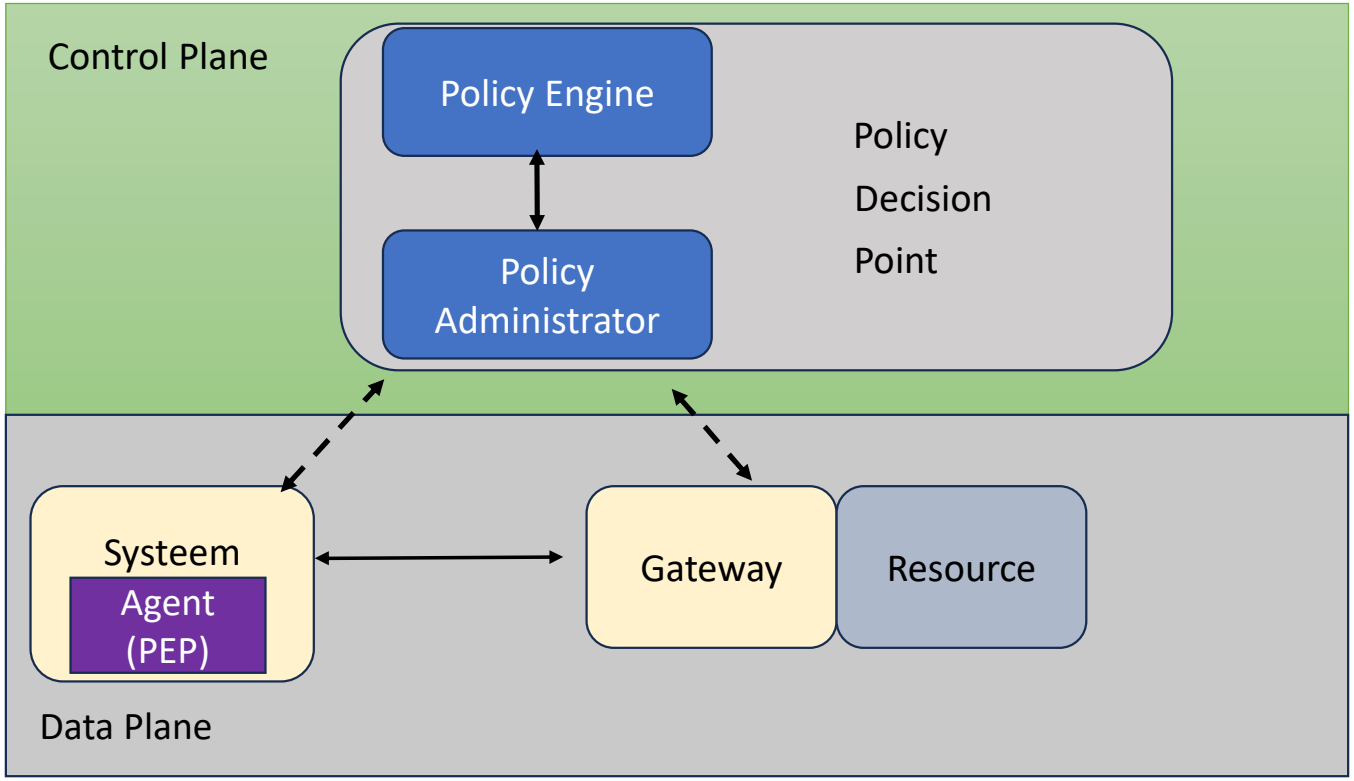


# Zero Trust User Access

*Conditional Access to Resources*



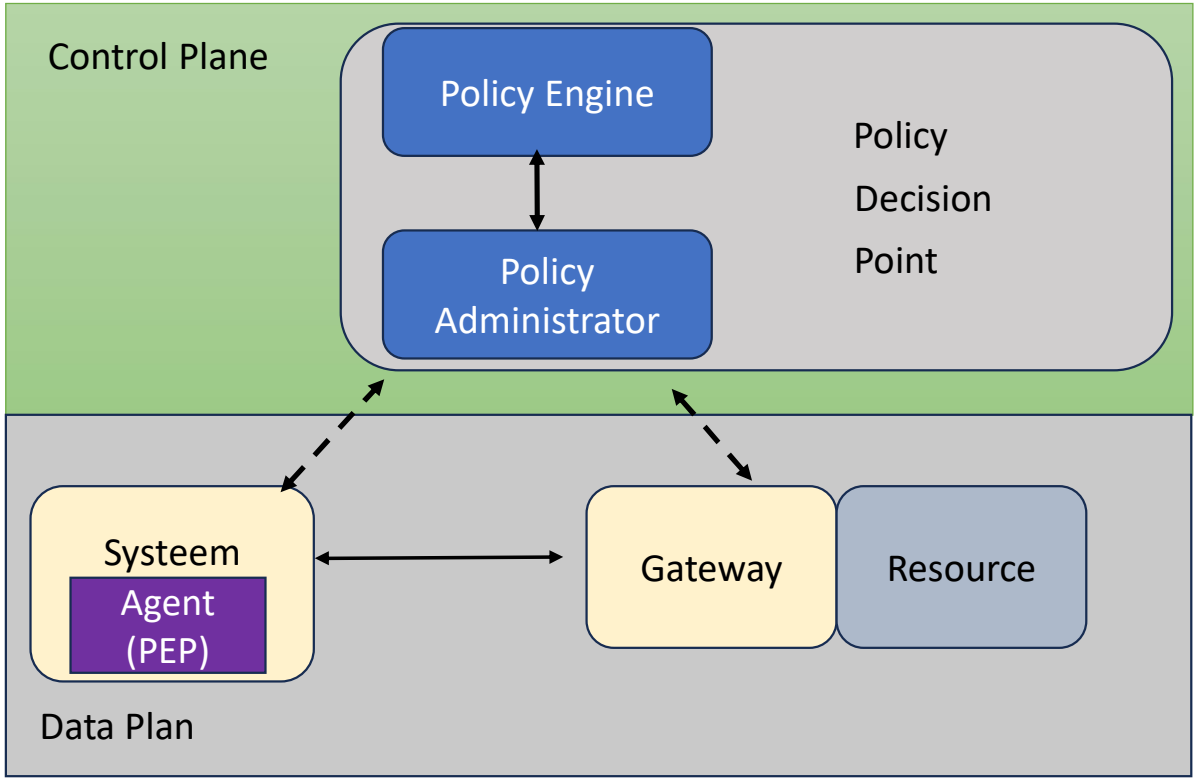
# Deployment model




## Deployment model details

- De PEP agent staat op alle systemen
- De PEP agent communiceert met de PA
- Als de PE het goedkeurd dan zet de PA een communicatie kanaal op tussen de PEP en de resource gateway

# Algoritmes en beleidsfundamenten




## Deployment model details

- PE is het centrale systeem van het PDP
- PE gebruikt trust algoritme om toegang toe te staan of te weigeren
- PE gebruikt data uit meerdere systemen en de policy database
- Policy DB:
  - Subject informatie
  - Subject attributen en rollen
  - Historische gedragspatronen
  - Threat intel
  - Metadata bronnen

# ZTA en Attribute gebaseerde toegang ABAC

Toegang wordt verleend op verschillende attributen en informatie uit verschillende bronnen.

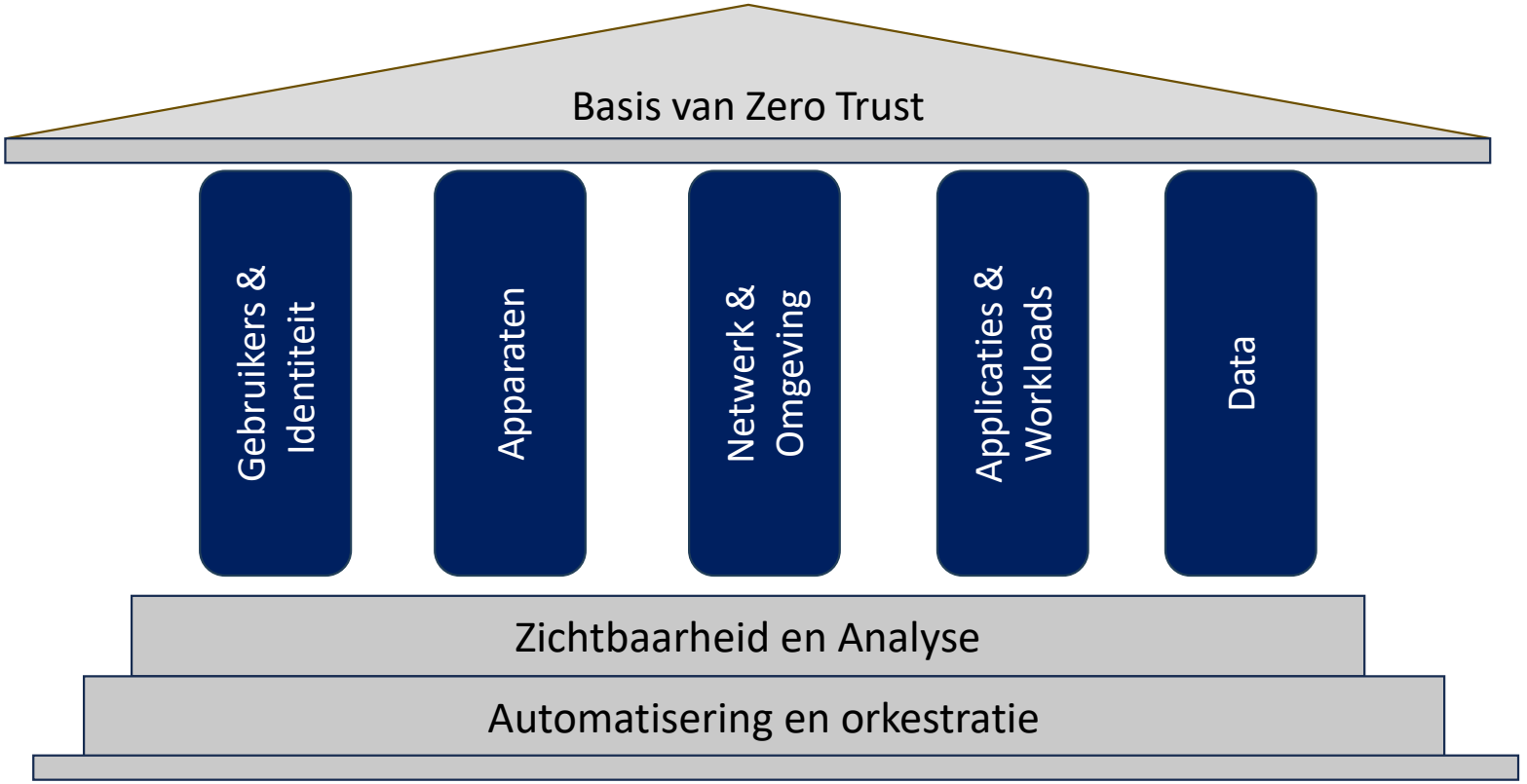
| Rollen (RBAC) | Attributen (ABAC) |
| --- | --- |
| • Rol<br>• Groepslidmaatschap | ▪ Tijd<br>▪ Locatie<br>▪ Operating Systeem<br>▪ Authenticatie geschiedenis<br>▪ Systeem configuratie<br>▪ Malware signatures<br>▪ Etc |

## *Kipling methode voor de ontwikkeling van policies*

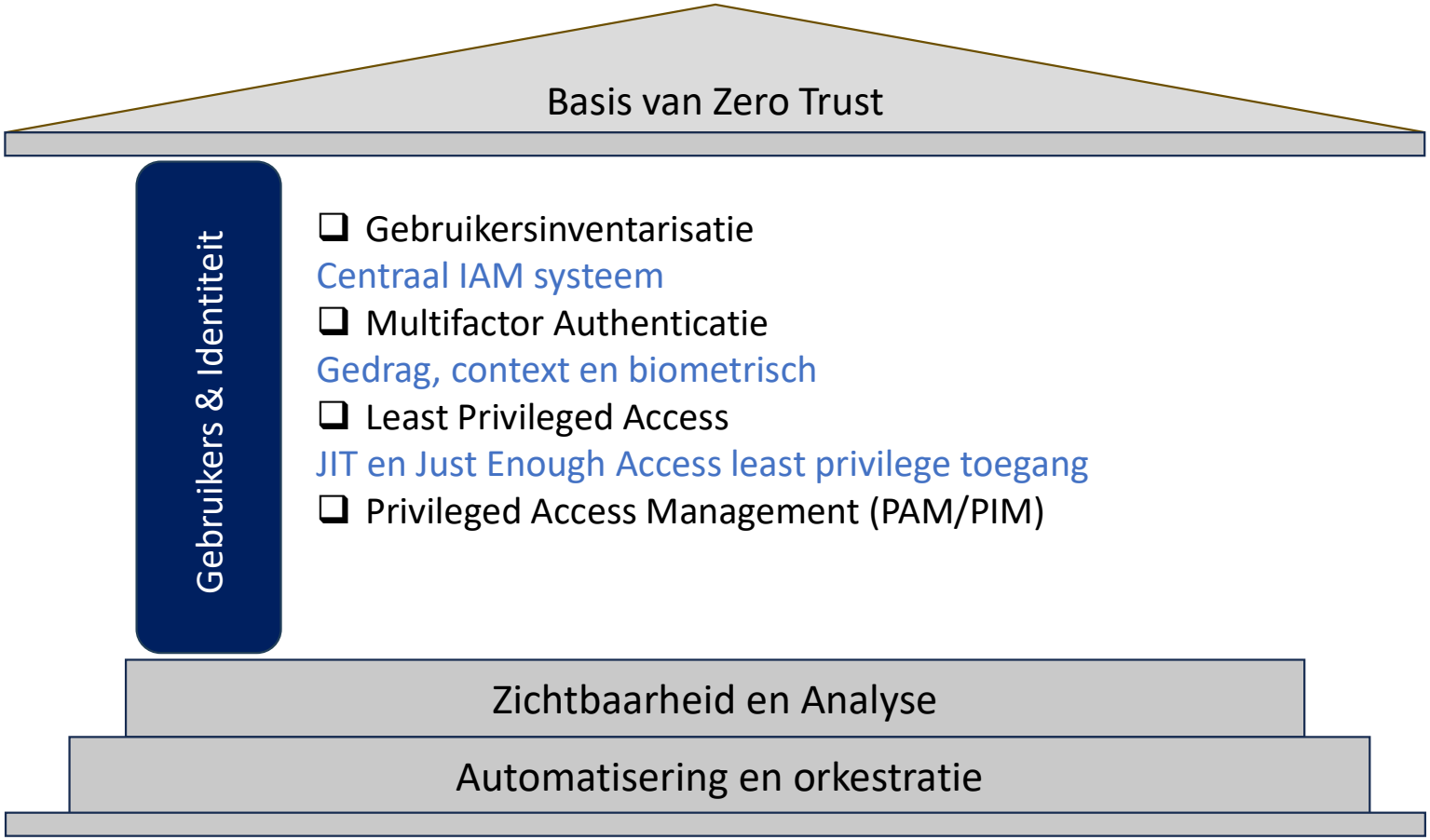
- Wie vraagt toegang
- Wat, tot welke applicatie wil men toegang
- Wanneer, wordt toegang gevraagd
- Waar vandaan het toegangsverzoek
- Waarom komt het toegangsverzoek
- Hoe zou toegang toegestaan moeten worden

| Wie | Wat | Waar | Wanneer | Waarom | Hoe |
|---|---|---|---|---|---|
| UserID | ApplicatieID | Apparaat<br>Locatie | Tijdstip | Classificatie<br>Data ID | Inhoud<br>Methode<br>Dreigingsbescherming |

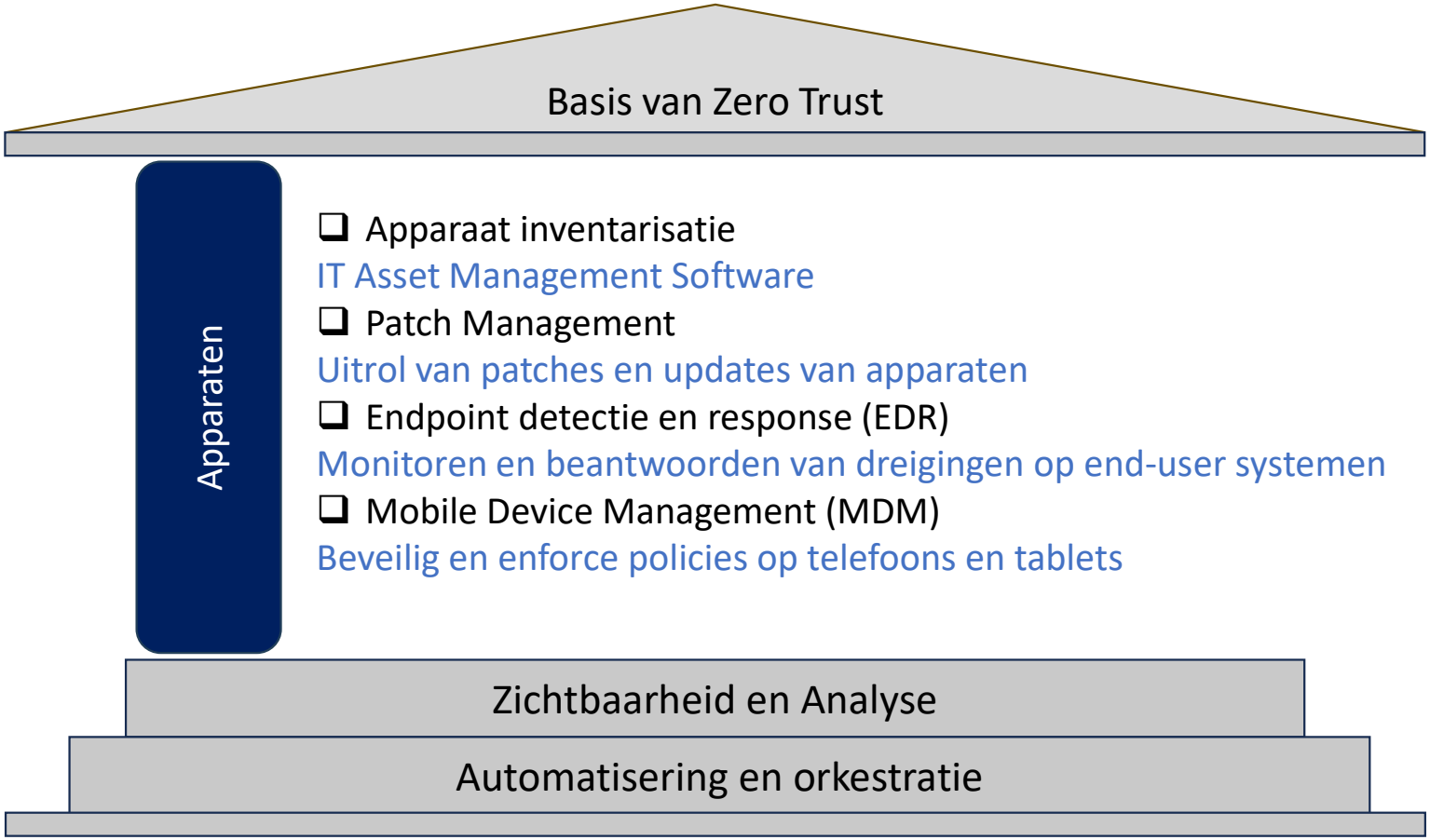
# Zero Trust Pilaren



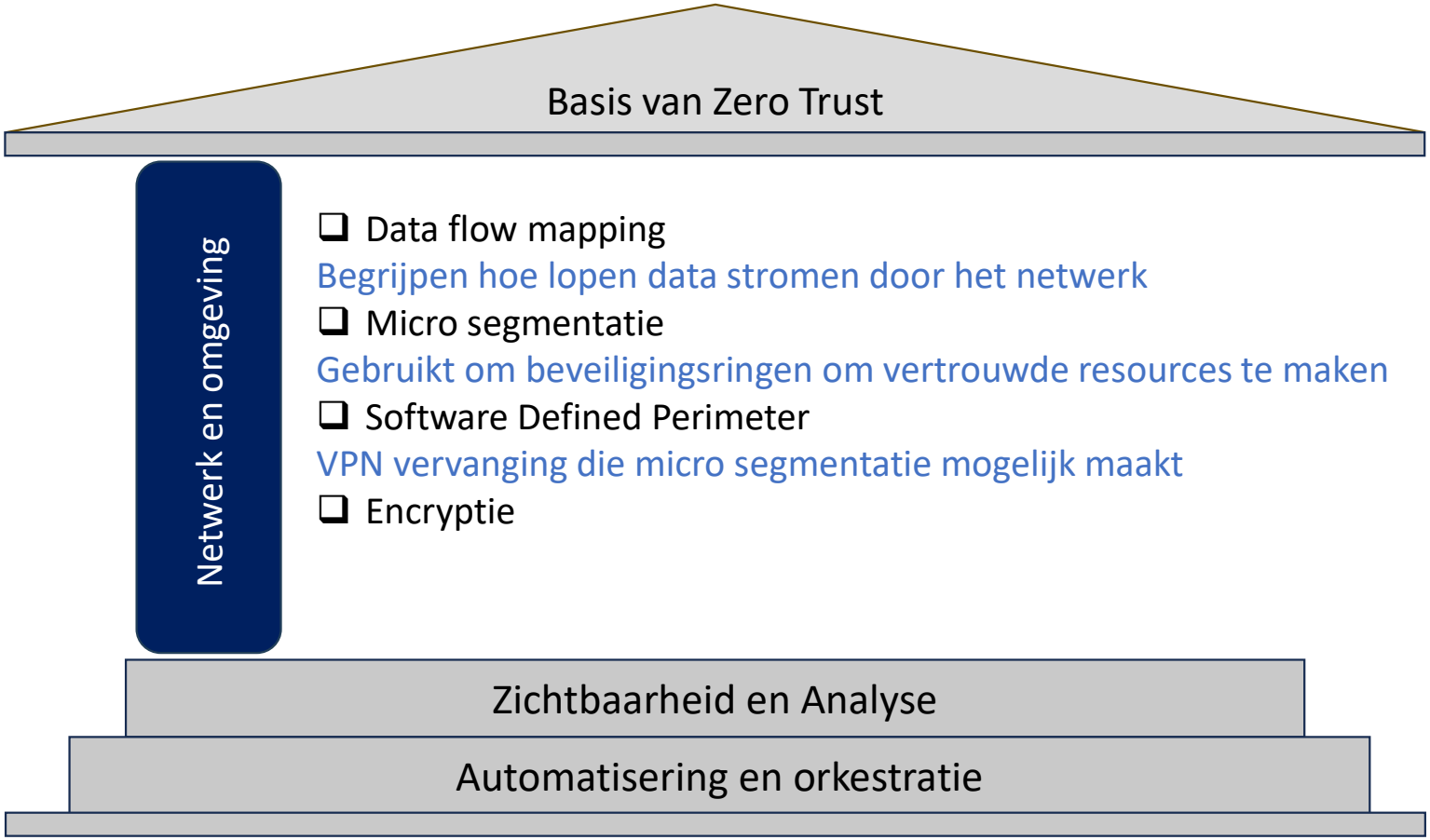
# Beveiligen van de gebruikers en identiteitspilaar



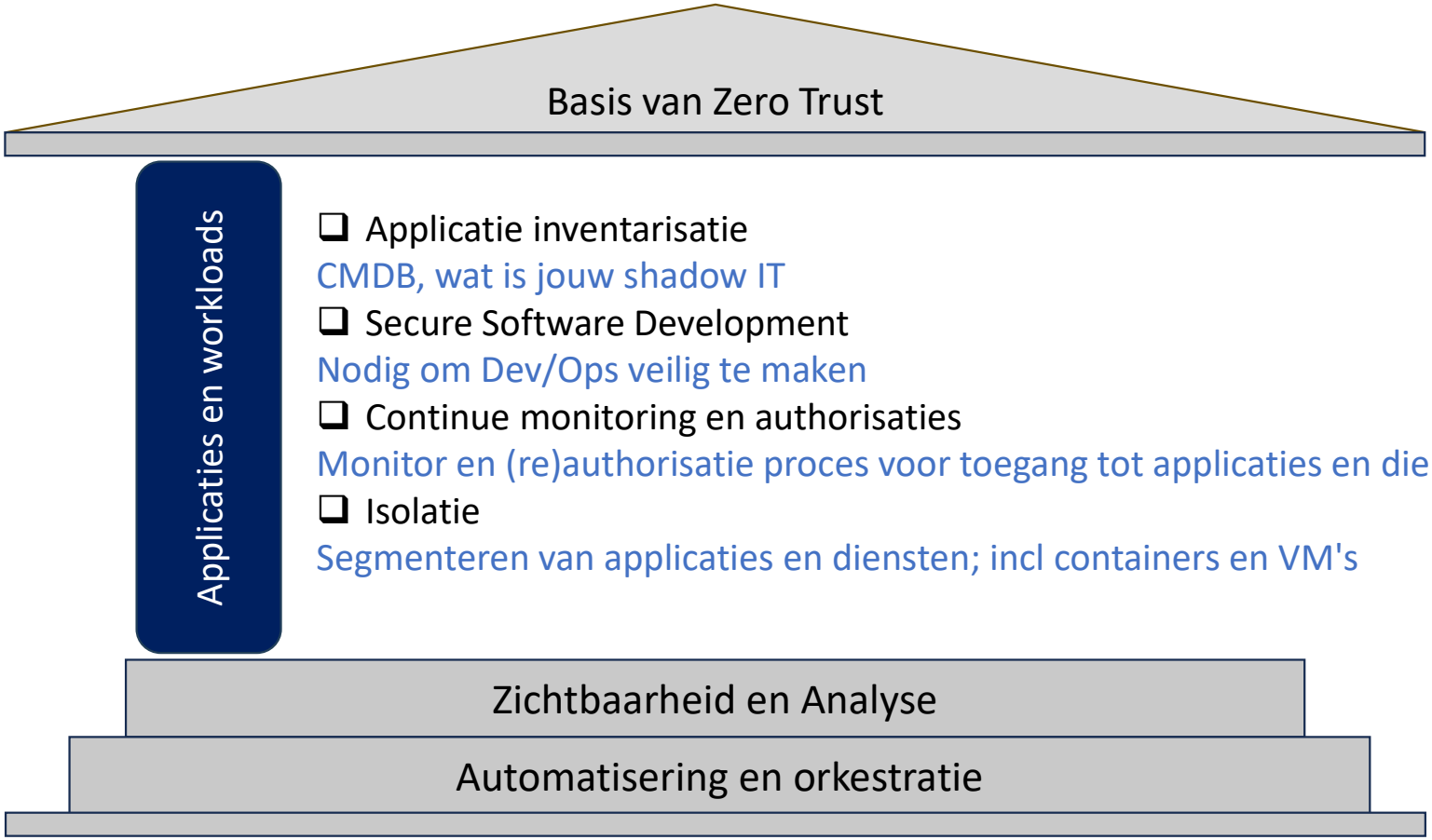
# Beveiligen van apparaten pilaar



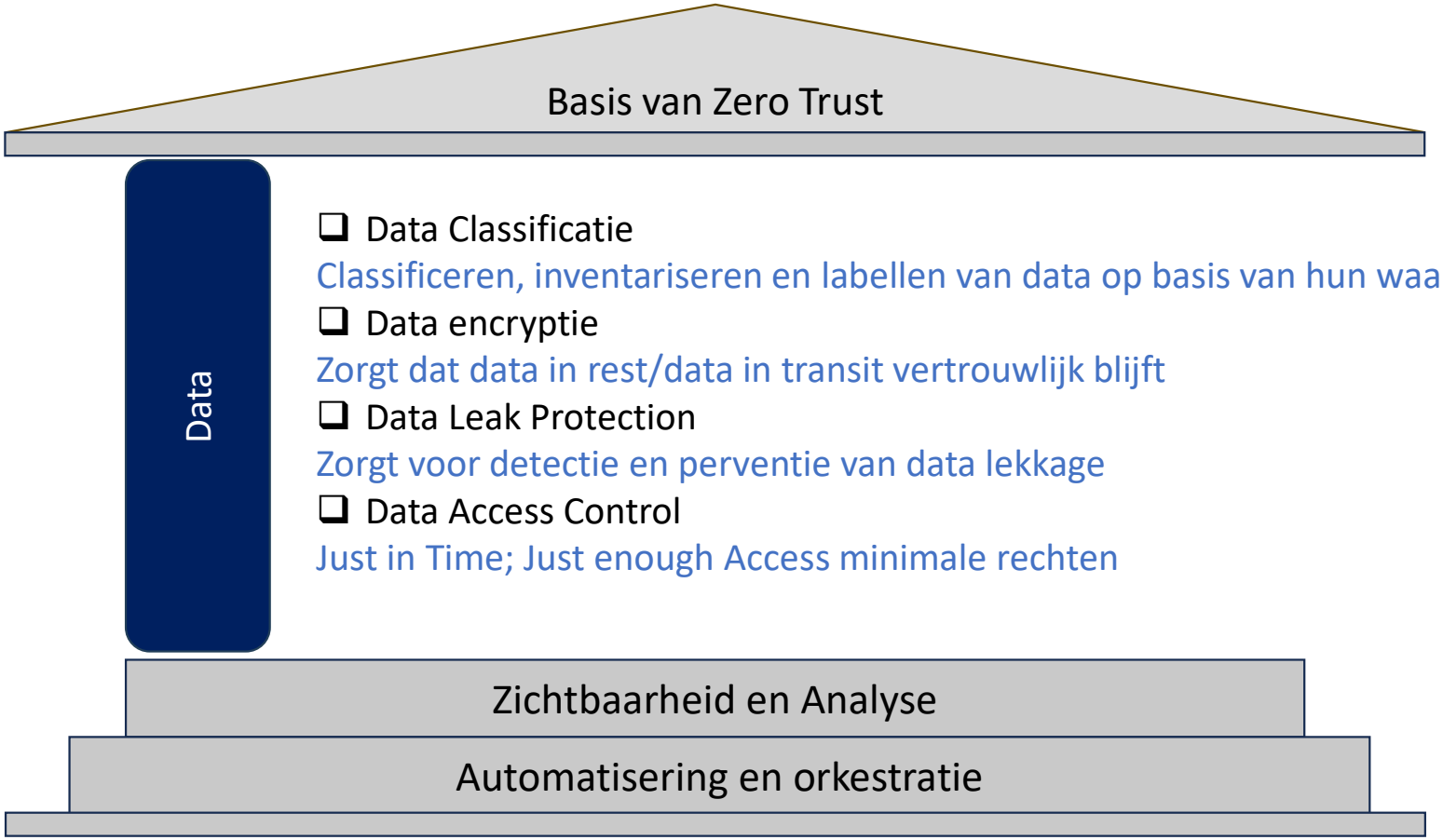
# Beveiligen van de netwerk pilaar



# Beveiligen van de netwerk pilaar



# Beveiligen van de data pilaar



# Zichtbaarheid en analyse


- ❑ Log al het verkeer

Al het verkeer wordt opgeslagen in een centraal log management systeem

- ❑ Continue monitoring

Monitor de omgeving op dreigingen

- ❑ Dreigingsanalyse

Informatie over cyber dreigingen, malware, kwetsbaarheden, zero-days

- ❑ SIEM

Verzamel en analyseer data en logs uit verschillende bronnen

# Automatisering


- ❑ Machine Learning en Artificial Intel

Maakt automatisering, snelheid en wentbaarheid in ZT mogelijk

- ❑ Security Orchestration, Automation en Response (SOAR)

Automatiseer IT security processen

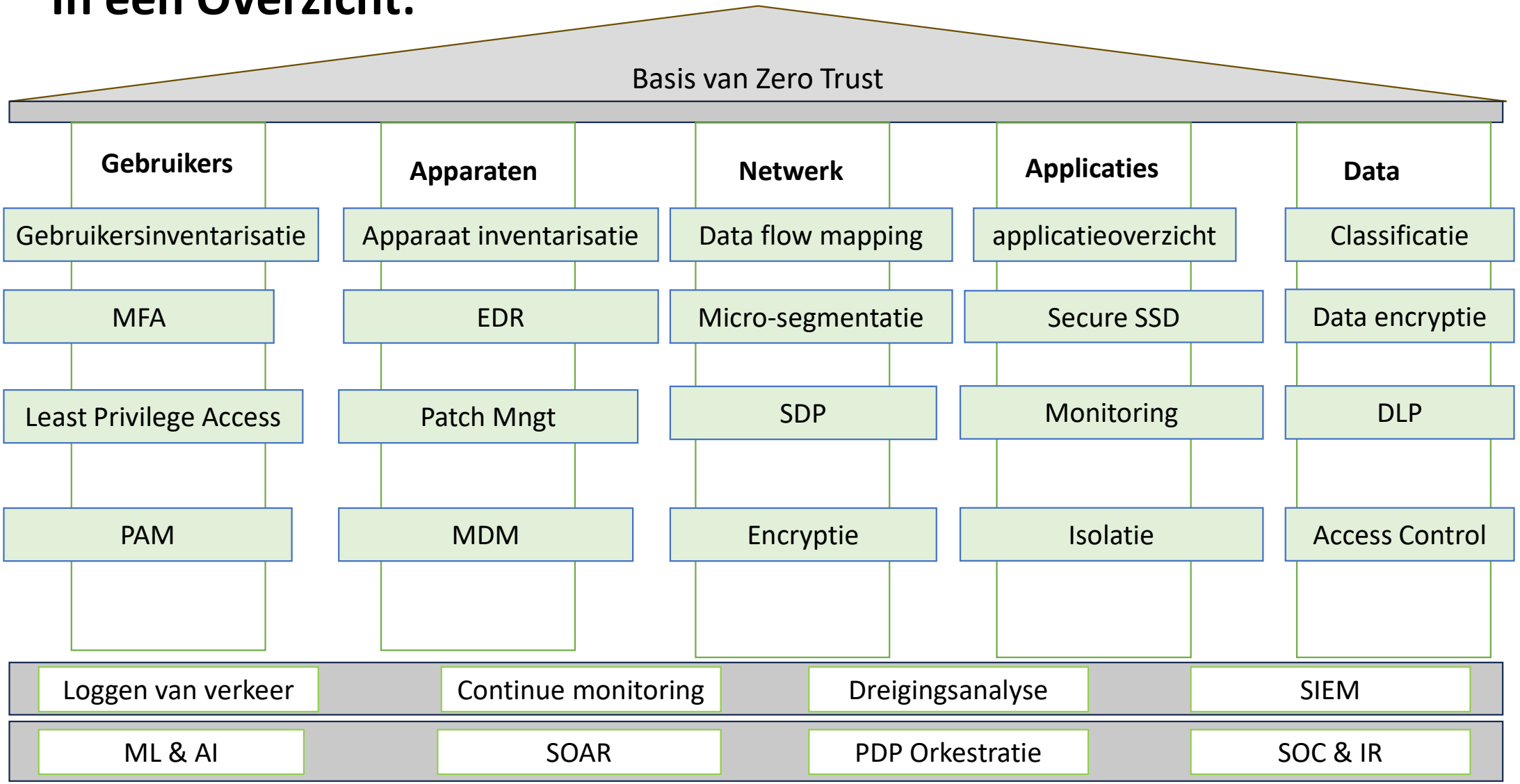
- ❑ PDP Orchestration

Zorgt voor integratie van lossen ZT architectuur data bronnen

- ❑ SOC & Incident response (IR) Integratie

Versnelt reactietijden op incidenten en verminderd false positives

# In een Overzicht:



# Ontwerp een Zero Trust Architectuur

# Vier ontwerp principes Zero Trust

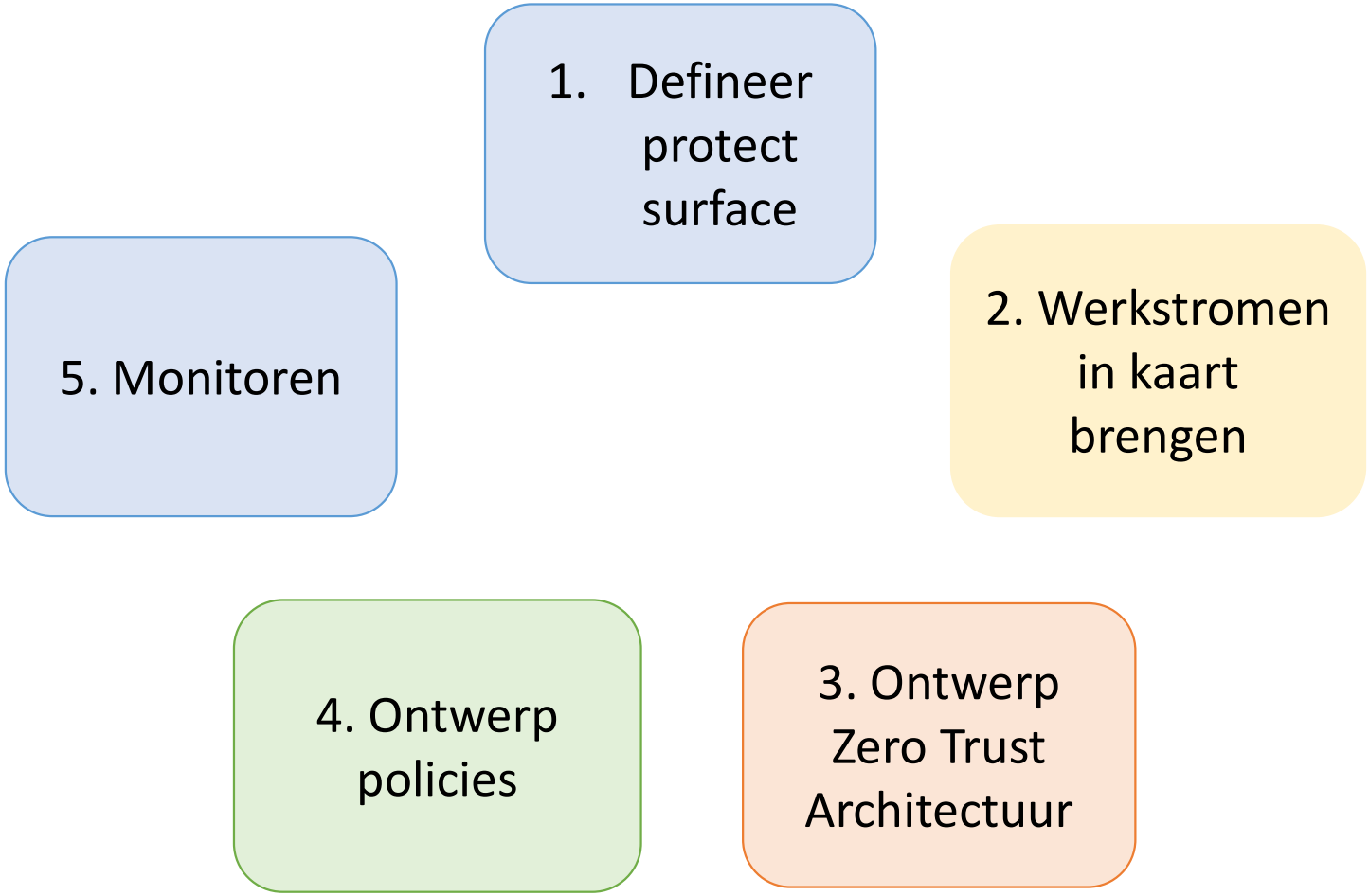
Business waarde

Van binnen naar buiten.
DAAS

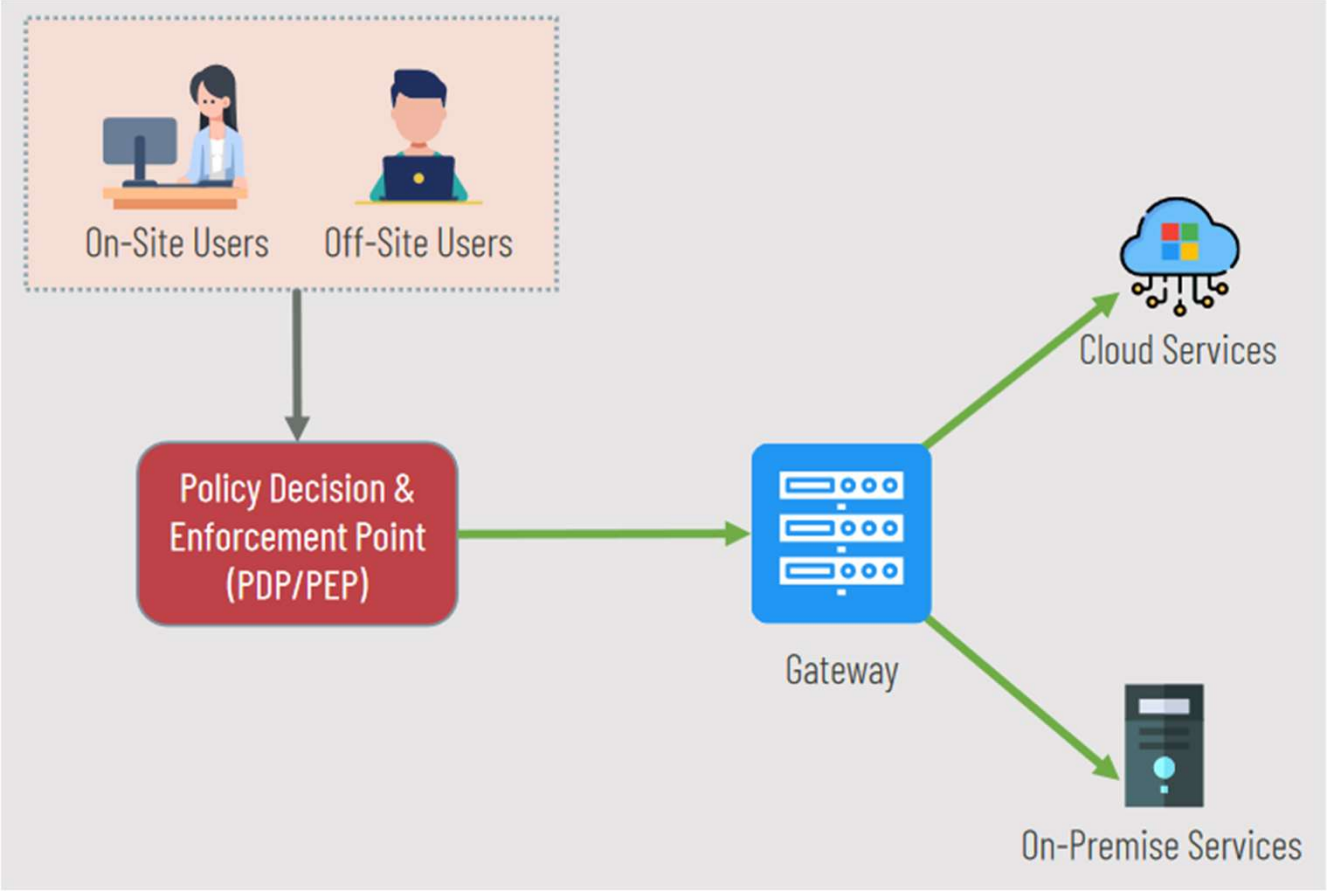
Wie mag waar bij

Monitor en log verkeer

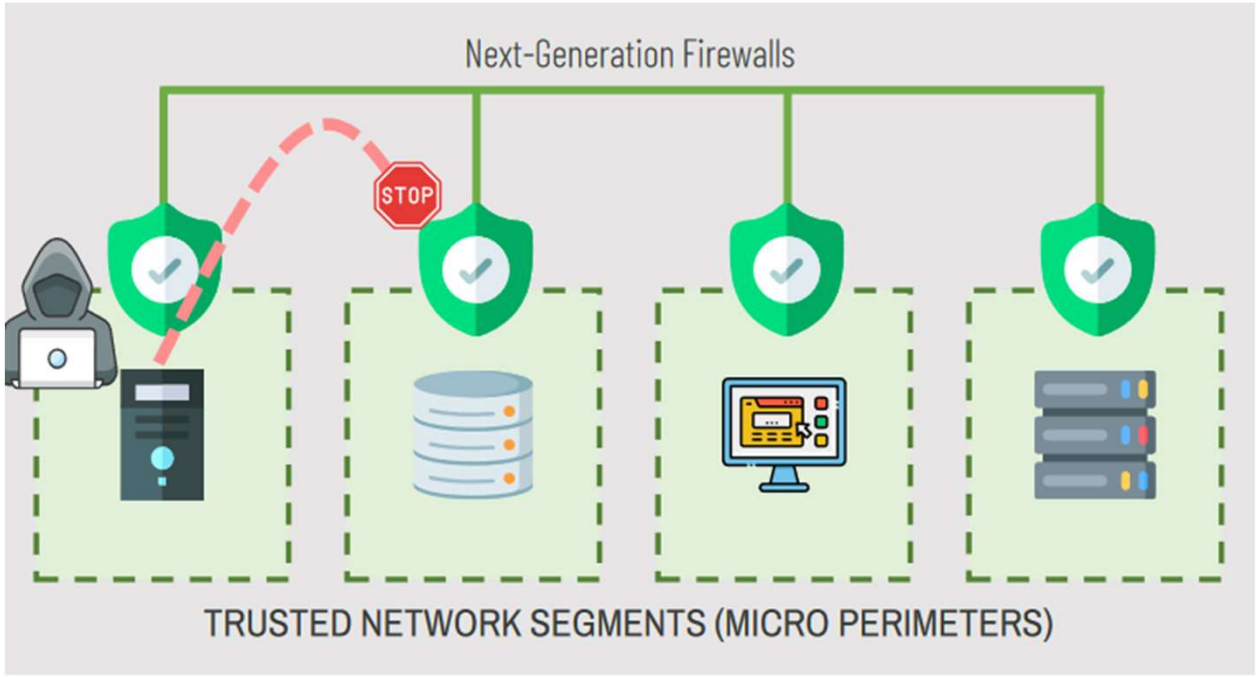
# Ontwerp methode Zero Trust



# Use cases


On-Site Users
Off-Site Users
Policy Decision & Enforcement Point (PDP/PEP)
Gateway
Cloud Services
On-Premise Services

# Stop lateral movement



# Altijd veilige toegang