# Vertrouw niets, Controleer alles

Beveiligen van de digitale ruimte in een wereld waarin alles met alles verbonden is


IT
VPN

# Verschuivende bedreigingen en grenzen

- De tijd dat data zich enkel binnen de muren van systemen bevindt is radicaal voorbij
- Alle bestaande IT-grenzen zijn nagenoeg vervaagd
- Van netwerk perimeter beveiliging naar Zero-Trust en identiteit beveiliging
- Alles is data, alles is software, alles gevirtualiseerd
- Strategische infrastructuur draagt bij aan data centrisch perspectief

# Eigenschappen Digitale Ruimte

- Een gemengde architectuur
  - Concrete basis of infrastructuur met virtuele uitbreidingen
- Een interface architectuur
  - Naar technische componenten binnen dezelfde infrastructuur als in verbinding met mensen en technologie buiten de eigen infrastructuur
  - Actieve input- en outputstromen
- Architectuur van onderlinge verbindingen
  - Hoofddoelstelling niet inhoud statisch herbergen maar functioneren als uitwisselingssysteem (of verbindingssysteem) tussen hier en elders.
  - Het hier is net zo grenzeloos zoals elders dat ook is….

# Ontwerpprincipes ZT-Architectuur

- Identificeer de te beschermen onderdelen van de IT-infrastructuur en beveilig alle paden er naartoe.
- Verschaf alleen toegang tot informatie via beveiligde verbindingen, ongeacht de locatie.
- Handhaaf strikte toegangscontrole op een need-to-know-basis.
- Bepaal de toegangsrechten op basis van mate van vertrouwen die afgeleid wordt uit verschillende eigenschappen van de toegangsaanvraag: account, apparaat, IP-adres en locatie.
- Zorg voor uitgebreide monitoring en logging.

# Algemene architectuurprincipes

- Controleer alle identiteits- en toegangsverzoeken tot gegevens voordat u toestemming geeft. Vertrouw nooit maar verifieer.
- Neem beslissingen op basis van transactierisico, geef nooit toegang uitsluitend op basis van netwerk plaats.
- Log en monitor zoveel mogelijk informatie.
- Microsegmentatie om beveiligingsrisico's in te dammen.
- Pas automatisering en orkestratie toe om routinematige beveiligingstaken te vereenvoudigen en te automatiseren om consistentie van uitvoering verbeteren.

# Logische core componenten Zero Trust (nist)

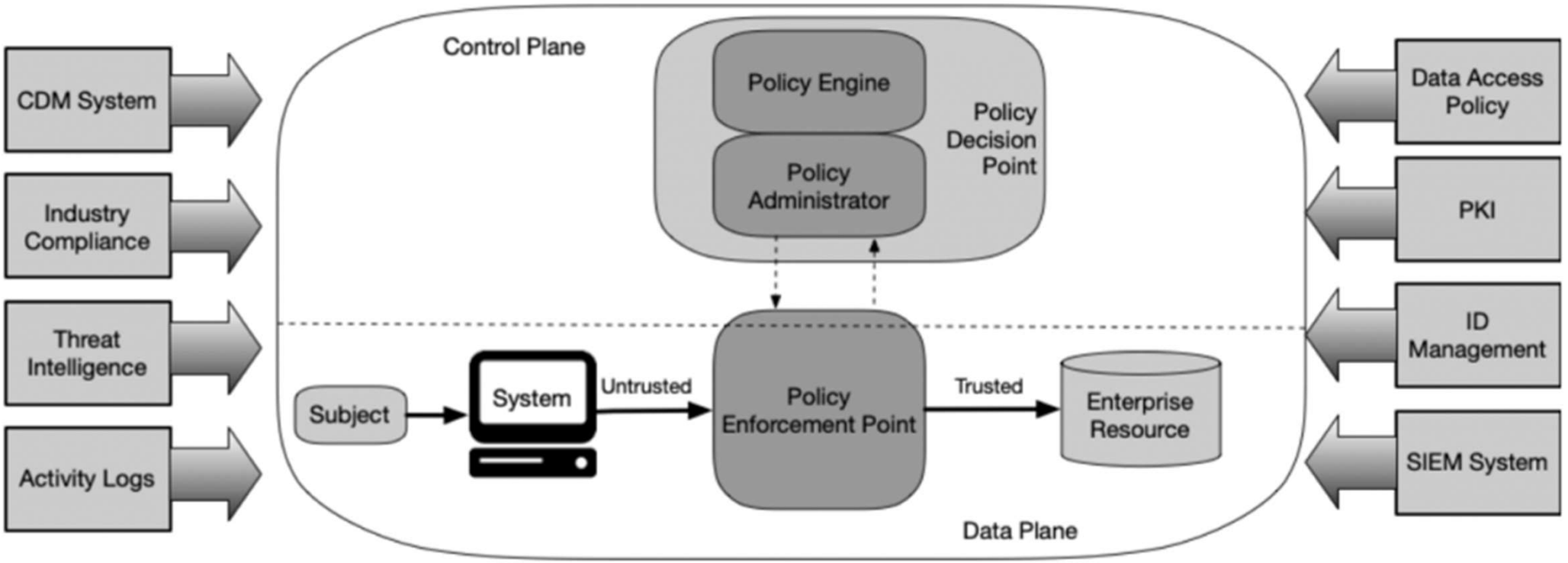



**Figure 2: Core Zero Trust Logical Components**

# Advies actieplan;

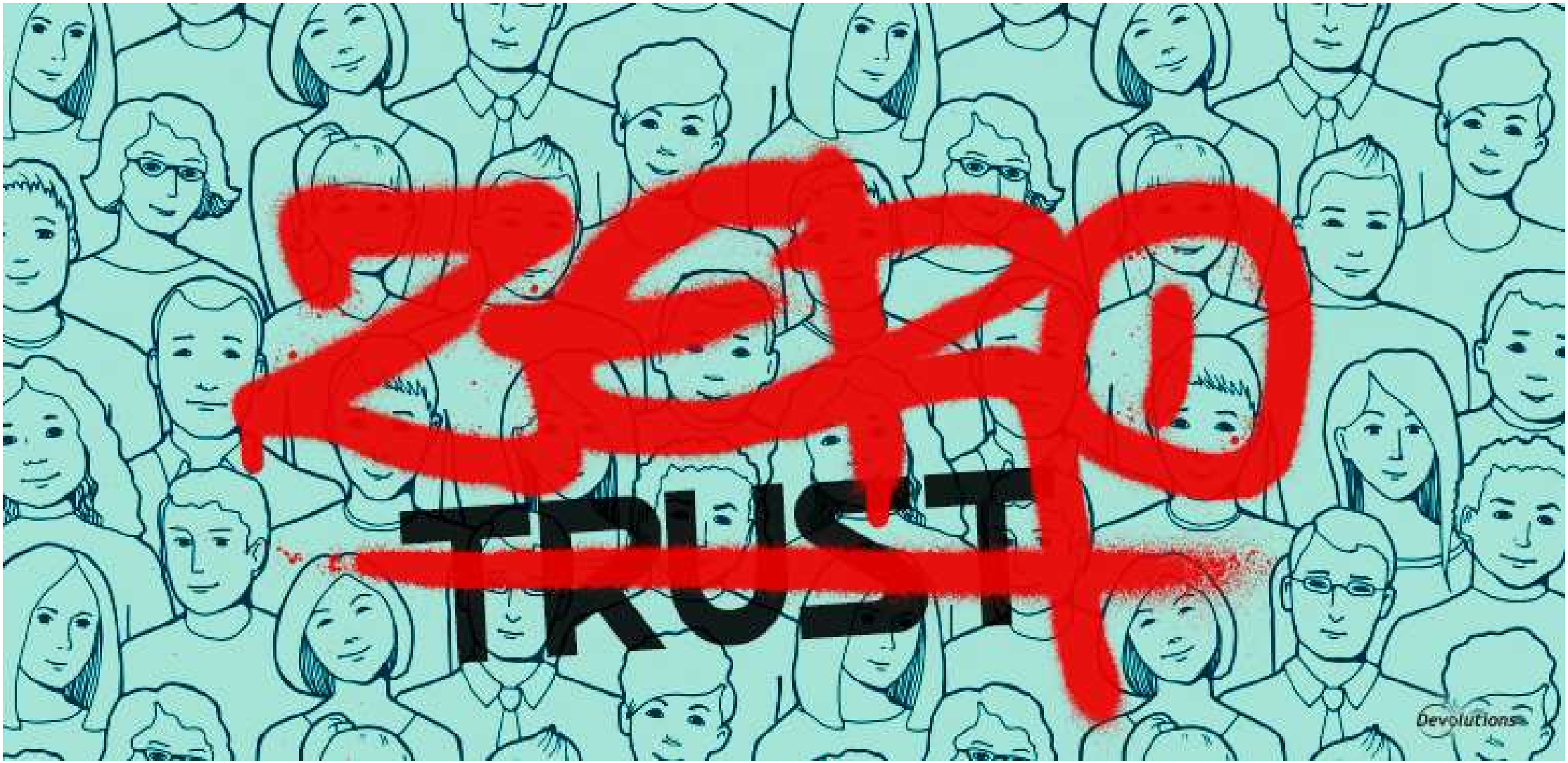
- Baseer het actieplan op de strategische doelen van uw organisatie en de uitkomsten van een risicoanalyse.
- Definieer een visie en missie waarin de doelen, resultaten en architectuur duidelijk zijn vormgegeven.
- Gebruik het actieplan om de leiding van uw organisatie mee te krijgen door u te richten op de doelen en resultaten die uw organisatie voor ogen heeft.
  - Op deze manier krijgt u ondersteuning voor uw eigen doelen, budgettoewijzingen en interne afstemming.
- Stel eindgebruikers in staat om mee te denken over de implementatie van Zero Trust.
  - Beveiliging zo inrichten dat die niet nadelig is voor hun gebruikerservaring en productiviteit. Als de maatregelen die Zero Trust toevoegt eindgebruikers hinderen, dan zoeken zij er een weg omheen en kunt u de voordelen van Zero Trust niet realiseren.
- Zoek indien nodig de samenwerking op met ICT- en securityleveranciers die bewezen expertise hebben in cloudgebaseerde beveiliging.

# Hoe beginnen?

1. Bepaal met welk onderdeel van uw infrastructuur u wilt beginnen.
2. Breng de transactiestromen in kaart op basis van de interacties van de in stap 1 geïdentificeerde DAAS-elementen.
3. Ontwerp eerst op papier een Zero Trust-omgeving en bouw daarna een proof-of-concept.
4. Ontwikkel het toegangsbeleid voor uw Zero Trust-omgeving vanuit de “Kipling-vragen”: wie, wat, wanneer, waar, waarom en hoe moet er al dan niet toegang verleend worden?
5. Bewaak en onderhoud het geheel door het analyseren van de informatiestromen van uw netwerk, systemen, applicaties en de cloud.

# Architectuur van de Digitale Ruimte

- Gemengde architectuur
- Interfacearchitectuur
- Architectuur van onderlinge verbindingen
- Van netwerk perimeter naar Zero-Trust en identiteit beveiliging
- Security- en defense architectuur


ZERO
TRUST
Devolutions