In Zero we Trust

Zero Trust bij NN Group

Floor van Eijk
Jeroen Eikema
René Kok
Linda de Boer

Agenda

- **Host: Linda de Boer – IT Development Manager Security**
- **Over NN Group: Floor van Eijk – CISO**
- **Wat is Zero Trust?: Jeroen Eikema – Security Architect**
  - Wat is het probleem?
  - Waarom willen we er iets aan doen?
  - Hoe ziet een Zero Trust oplossing er uit
- **Zero Trust bij NN Group: René Kok – Product Owner**
  - Zero Trust user access met Zscaler Private Access
  - Project aanpak: uitdagingen en successen

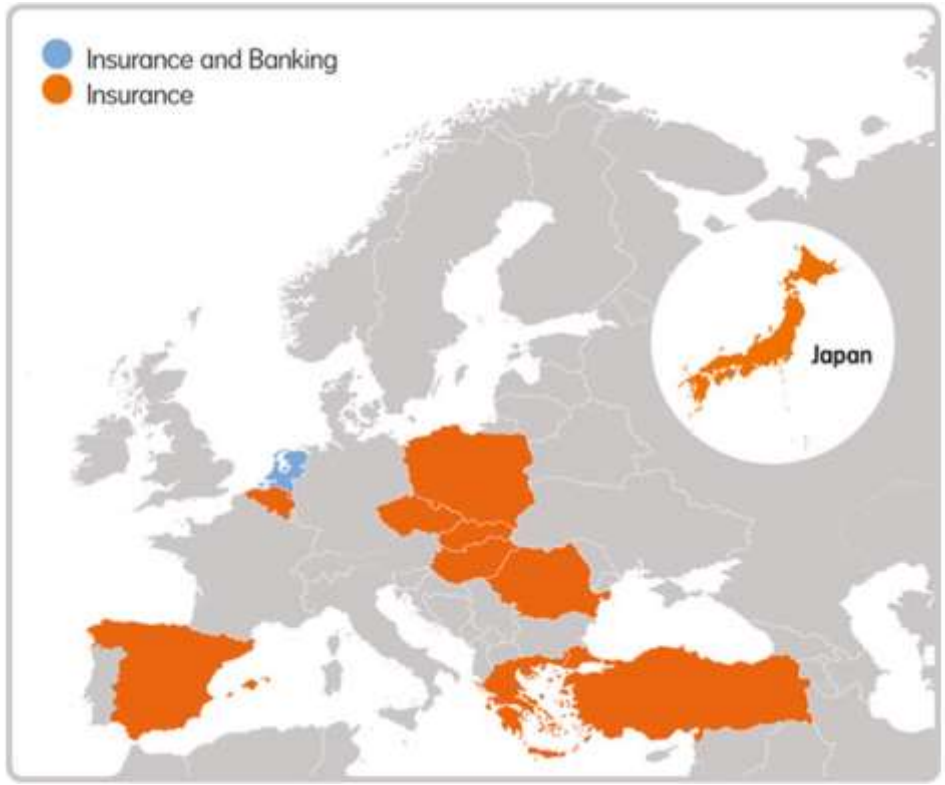
Over NN Group

Over NN Group

- Multinational met producten in pensioenen, verzekeringen, bankieren en investeren.
- Internationaal actief, hoofdkantoor in Den Haag

- Bijna 16.000 medewerkers, ~20 miljoen klanten

- Onze merken:



Our purpose

We help people care for what matters most to them

Our ambition

We want to be an industry leader, known for our customer engagement, talented people, and contribution to society

Our values

Care

Clear

Commit

Our brand promise

You matter

Our strategic commitments

Customers and distribution
We see our customers as the starting point of everything we do.

Products and services
We develop and provide attractive products and services.

People and organisation
We empower our colleagues to be their best.

Financial strength
We are financially strong and seek solid long-term returns for shareholders.

Society
We contribute to the well-being of people and the planet

Centrale Security functies

Enterprise Security Services

Access & Authentication

Ondersteunen van NN Group in het behouden van **vertrouwelijkheids- en integriteitslevels** voor alle identiteiten en hun (toegekende) toegang

Security Consultancy & Assurance

Onze product teams in staat stellen om hun **digitale producten veilig en betrouwbaar** te ontwikkelen en beheren, zodat klanten erop kunnen rekenen

Cyber Defense Centre

Zoeken naar, **detecteren en mitigeren van cyberaanvallen** “in every form, anytime and anywhere”

Cyber Testing Centre

Verbeteren van de **hardening** en **verminderen van het aantal vulnerabilities** binnen de hele NN Group organisatie

Wat is Zero Trust?

Agenda

- Introductie
- De geschiedenis tot nu
- Trends en ontwikkelingen
- Introductie van Zero Trust
- Definitie en doelstelling
- Zero Trust uitgangspunten
- Zero Trust modellen
- Zero Trust maturity model
- Zero Trust aanpak

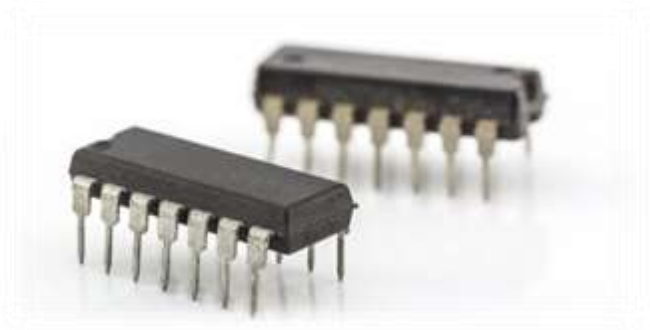
De Geschiedenis tot nu toe…

1940

1945: ENIAC

1950

1958: eerste geïntegreerde circuit



1960

1970

1968: eerste computer netwerk: ARPANET

1980

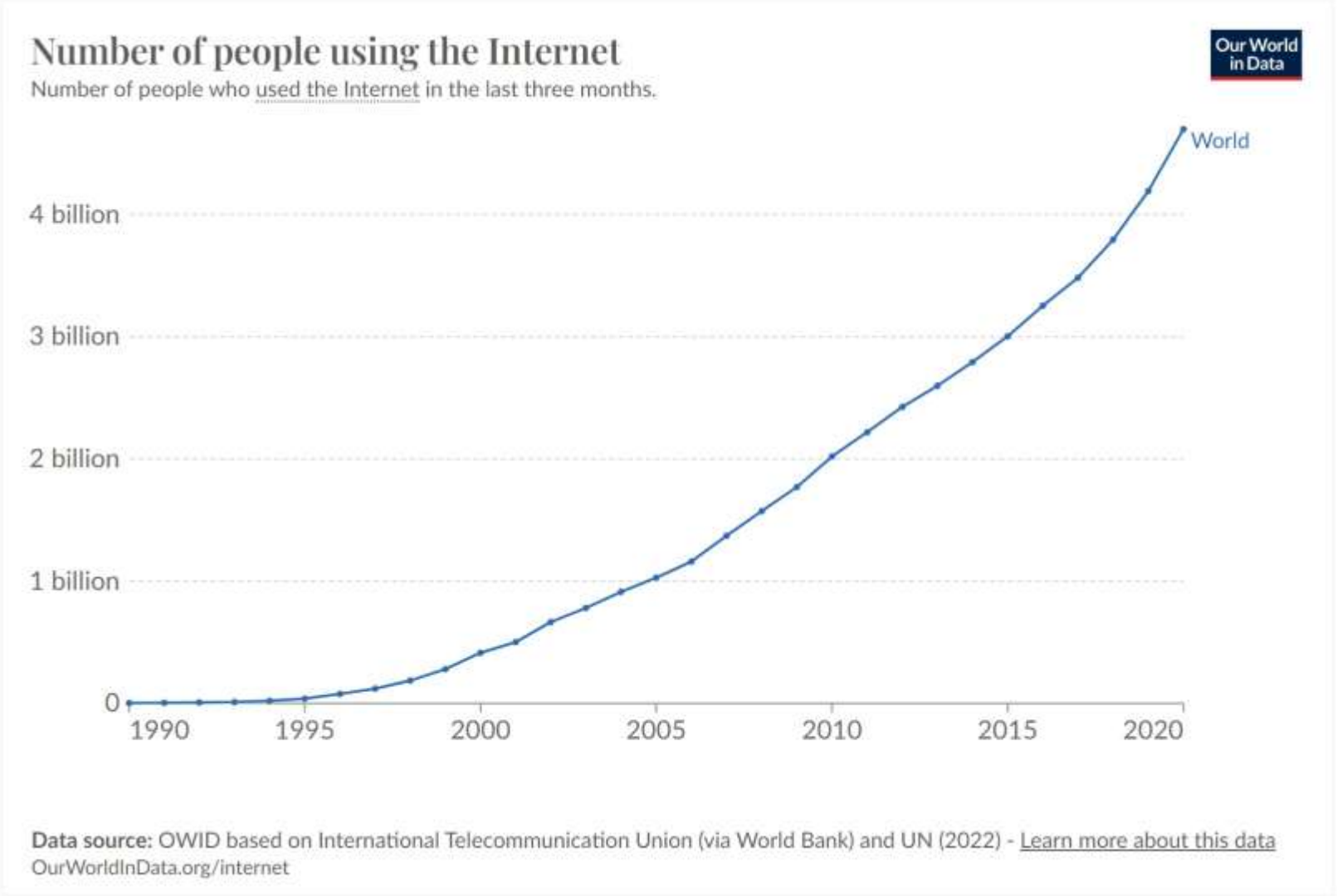
1983: geboorte Internet

1990

1993: commerciële openstelling internet

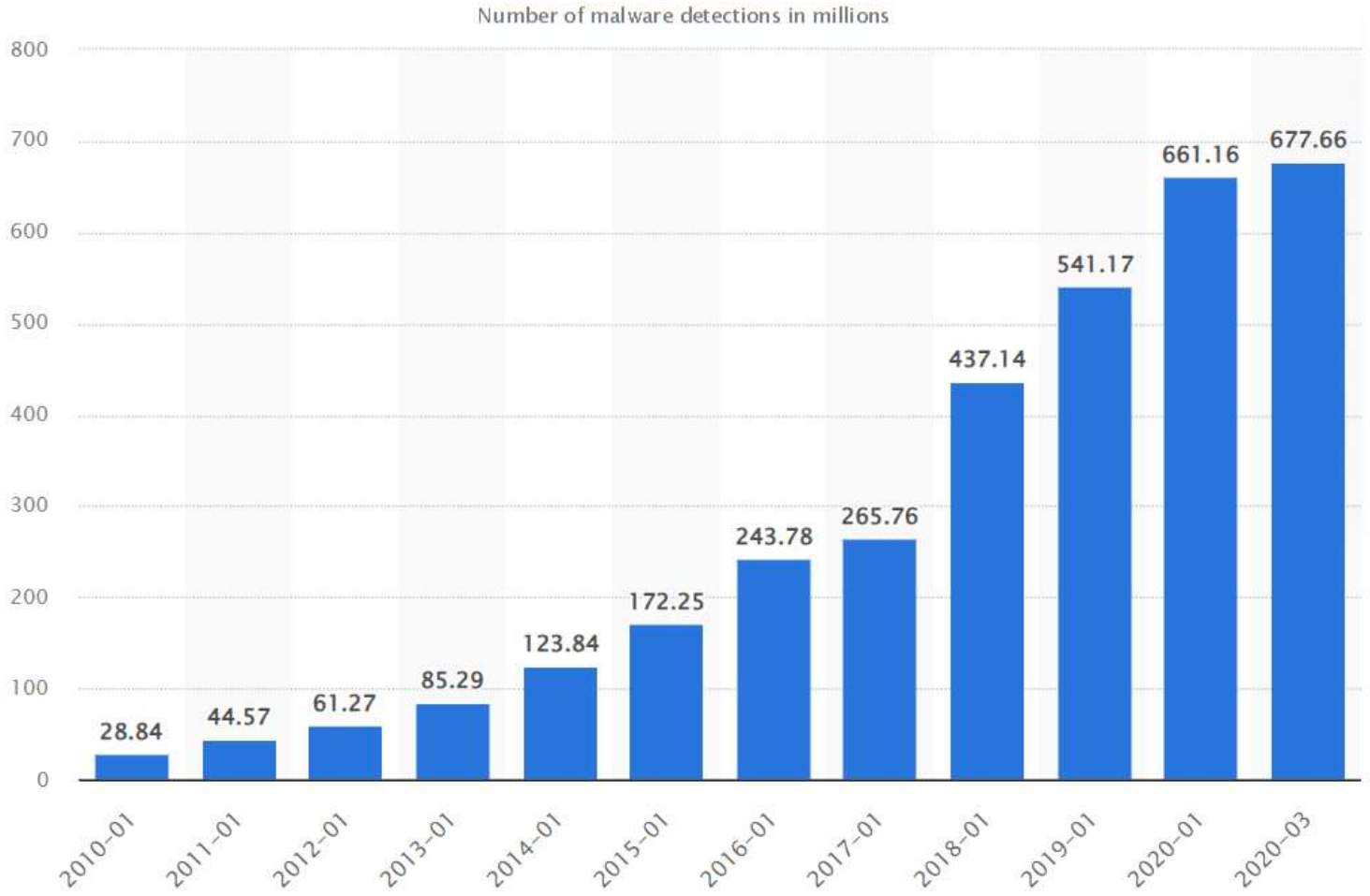
…vervolgens

- Inmiddels maakt ~5 miljard mensen regelmatig gebruik van het internet
- Het aantal aangesloten devices is waarschijnlijk een veelvoud hiervan



…en vervolgens

- De illustratie toont het aantal malware detecties in de periode 2010-2020
- De eerste malware stamt uit de jaren 70 en die “besmette” systemen op ARPANET
- Malware heeft zich ontwikkeld van relatief onschuldige test-software tot geduchte cyber wapens



Maatregelen

Het werd duidelijk dat maatregelen nodig waren om te beschermen tegen malware en privacy te waarborgen.

- Packet filtering
- Firewalls
- Proxies
- Gateways
- Netwerk segmentatie
- Netwerk zonering
- Microsegmentatie
- Anti-virus
- Anti-malware
- DMZ
- NAT
- SWG
- IDS
- IPS
- DLP
- NGFW
- NDR
- EDR
- XDR
- SSO
- MFA
- PKI
- HSM
- KMS
- SIEM

Ontwikkelingen die Cyber Security uitdagen

- Cloud
- IoT / OT
- Mobile
- Any, any, any
- Cyber threats

Resultaat…

- Het kasteel met slotgracht stond lange symbool voor cyber security
- Dit model is weliswaar hard van buiten, maar tegelijkertijd zacht van binnen
- Het is inmiddels duidelijk dat dit model ons niet verder brengt

Introductie van Zero Trust

- Jericho forum (2004): “de-perimeterization”
- John Kindervag (2010): basisgedachte is *never trust, always verify*
- Google BeyondCorp (2014): ontwikkeld voor veilige applicatie ontwikkeling voor Google medewerkers
- NIST Special Publication 800-207 (2020): Zero Trust Architecture
- CISA (2023): Zero Trust Maturity Model
- Executive Order 14028 (2021): federale diensten moeten een Zero Trust architectuur ontwerpen en implementeren

Zero Trust Definitie

Zero Trust Definitie

- Zero trust is een verzameling concepten en ideeën die zijn ontworpen om onzekerheid te minimaliseren, door bij ieder verzoek voor toegang tot informatiesystemen en diensten nauwkeurige, op least privilege gebaseerde besluiten af te dwingen, ervan uitgaande dat het netwerk is gecompromitteerd

Zero Trust Architectuur Definitie

- Een zero trust architectuur is het cyber security plan van een organisatie dat gebruikmaakt van zero trust concepten en dat relaties tussen componenten, werkprocessen en toegangsbeleid omvat

Zero Trust Doelstelling

- Het doel van Zero Trust is om ongeautoriseerde toegang tot data en diensten te voorkomen, door toegangscontrole zo granulair mogelijk te maken

De weg naar Zero Trust is een voortschrijden proces dat jaren kan duren

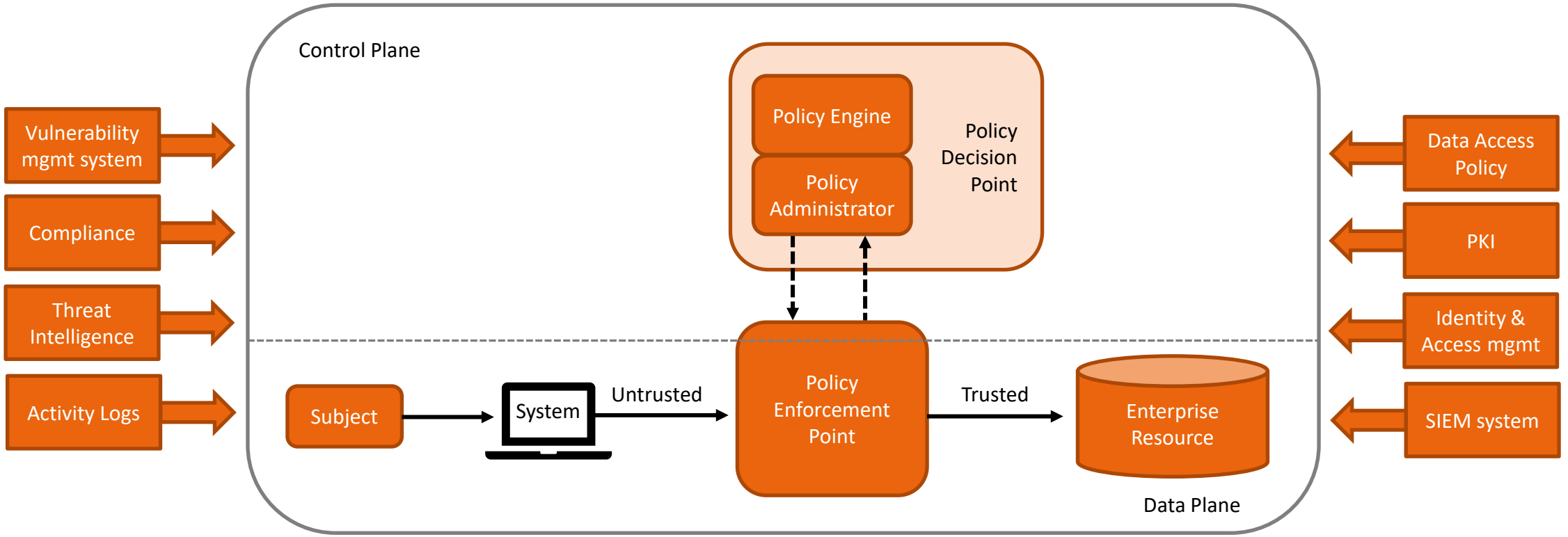
NIST Zero Trust Uitgangspunten

1. Alle databronnen en computerdiensten zijn **resources**
2. Alle communicatie wordt **beveiligd**, ongeacht het netwerk
3. Toegang tot individuele organisatie resources wordt **per sessie** verleend
4. Toegang tot resources wordt bepaald door **dynamisch beleid**
5. De organisatie monitort en bewaakt de **integriteit** en **security status** van al haar resources
6. **Authenticatie** en **autorisatie** voor toegang op alle resources wordt dynamisch uitgevoerd en strikt afgedwongen
7. De organisatie verzamelt zo veel mogelijk informatie over de **huidige status** van haar resources en gebruikt die om de security status te verbeteren

Uitganspunten Zero Trust Architectuur

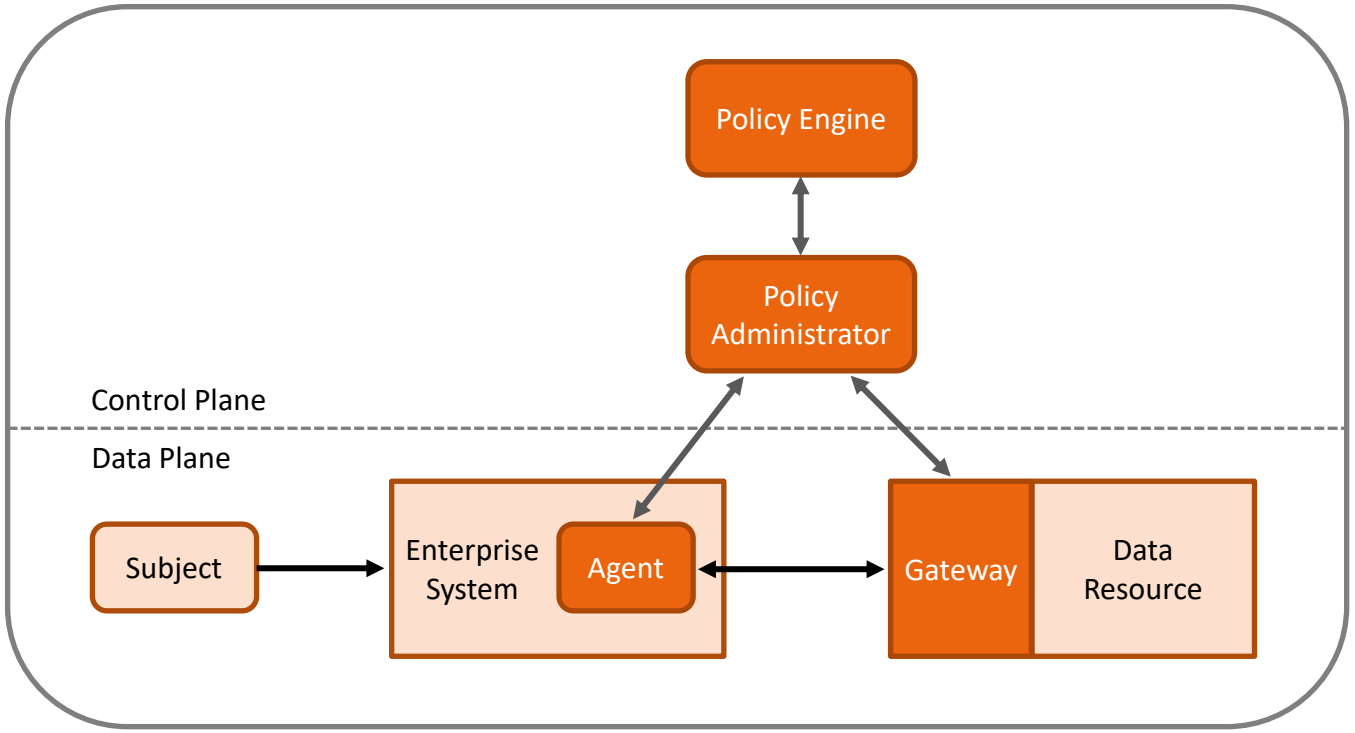
Risk based least privilege access

Diagram Zero Trust Oplossing



Bron: NIST 800-207

Device Agent / Gateway Model

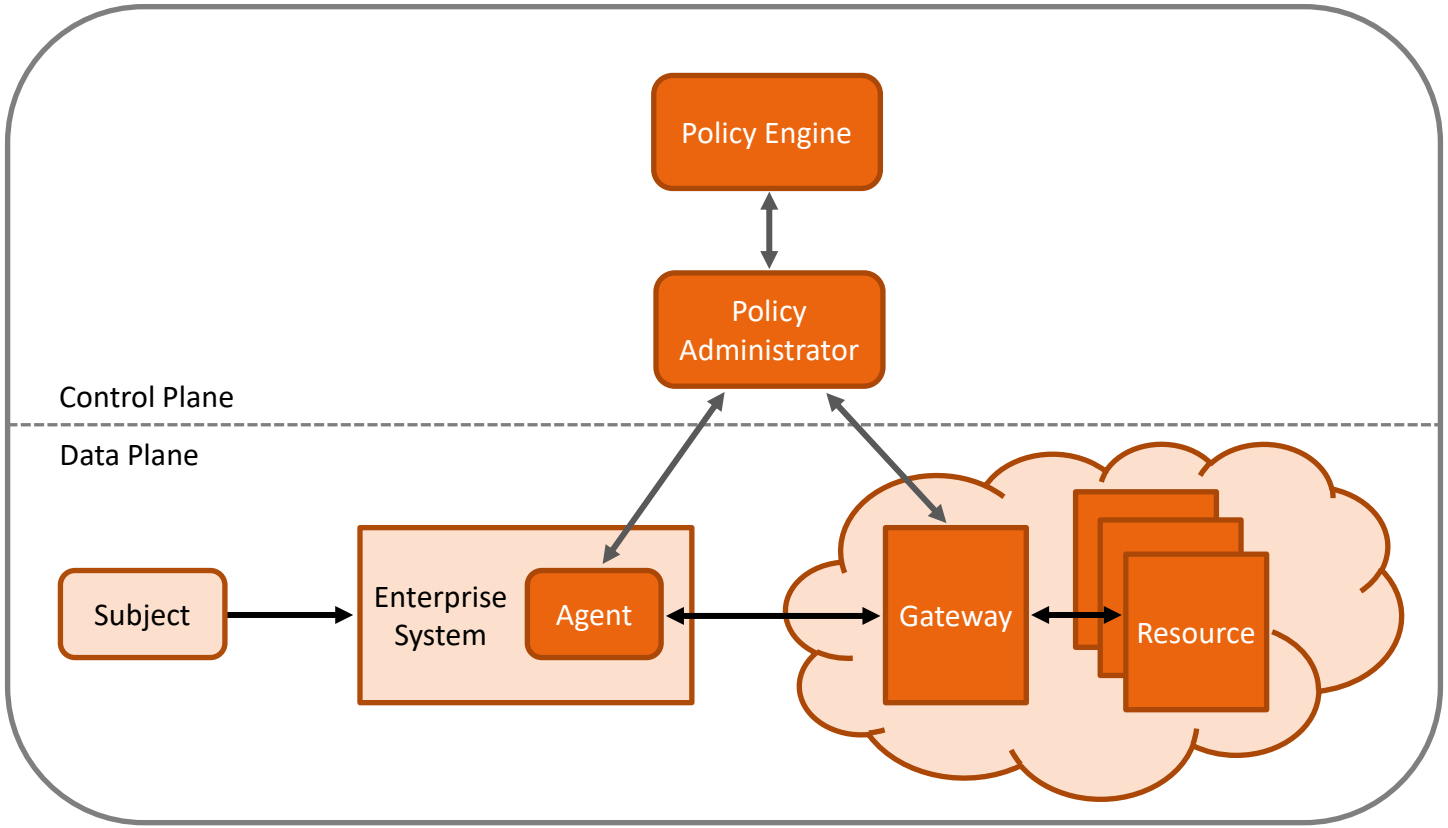


Karakteristieken:

- Toegang alleen mogelijk met een agent geïnstalleerd op het Enterprise systeem
- Vereist robuust device management
- De gateway fungeert als proxy voor de data resource
- Vereist een gateway die direct voor resources geplaatst kan worden
- Niet geschikt voor BYOD scenario's

Bron: NIST 800-207

Enclave-Based Deployment

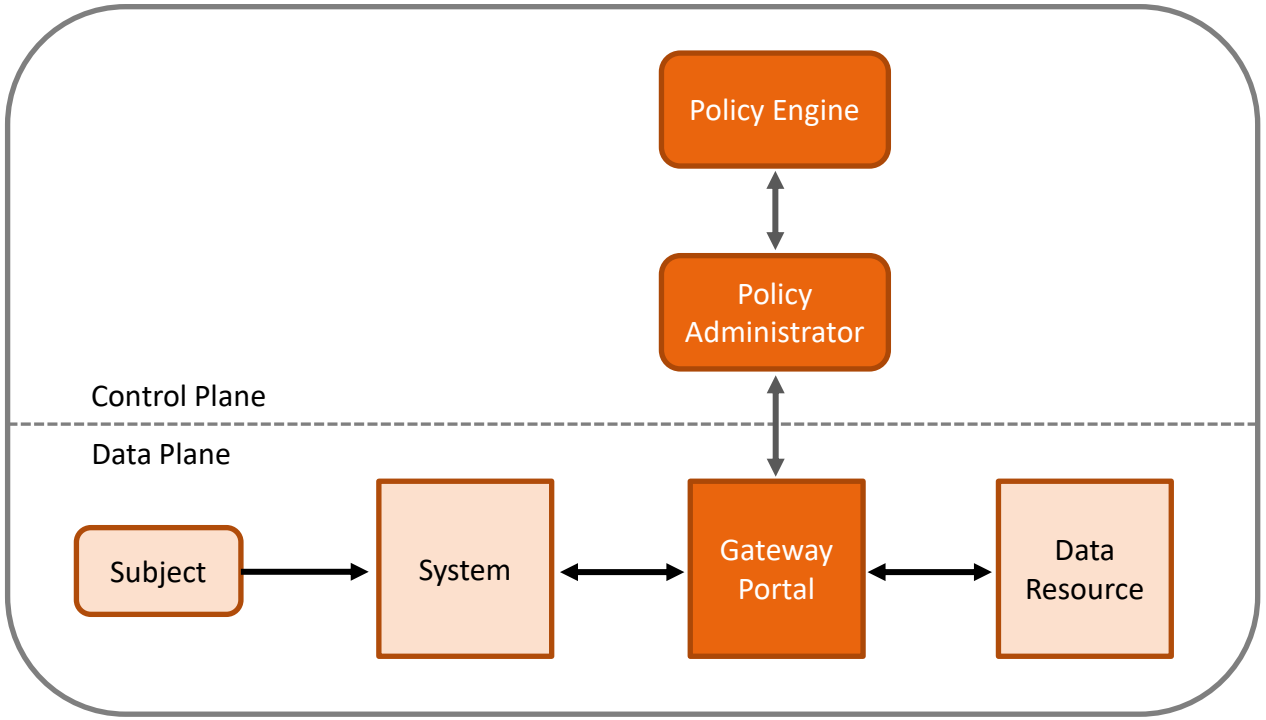


Karakteristieken:

- Toegang alleen mogelijk met een agent geïnstalleerd op het Enterprise systeem
- Vereist robuust asset en configuration management
- Beschermt verzamelingen resources
- Geschikt voor legacy applicaties
- Geschikt voor microservices in de cloud

Bron: NIST 800-207

Resource Portal-Based Deployment

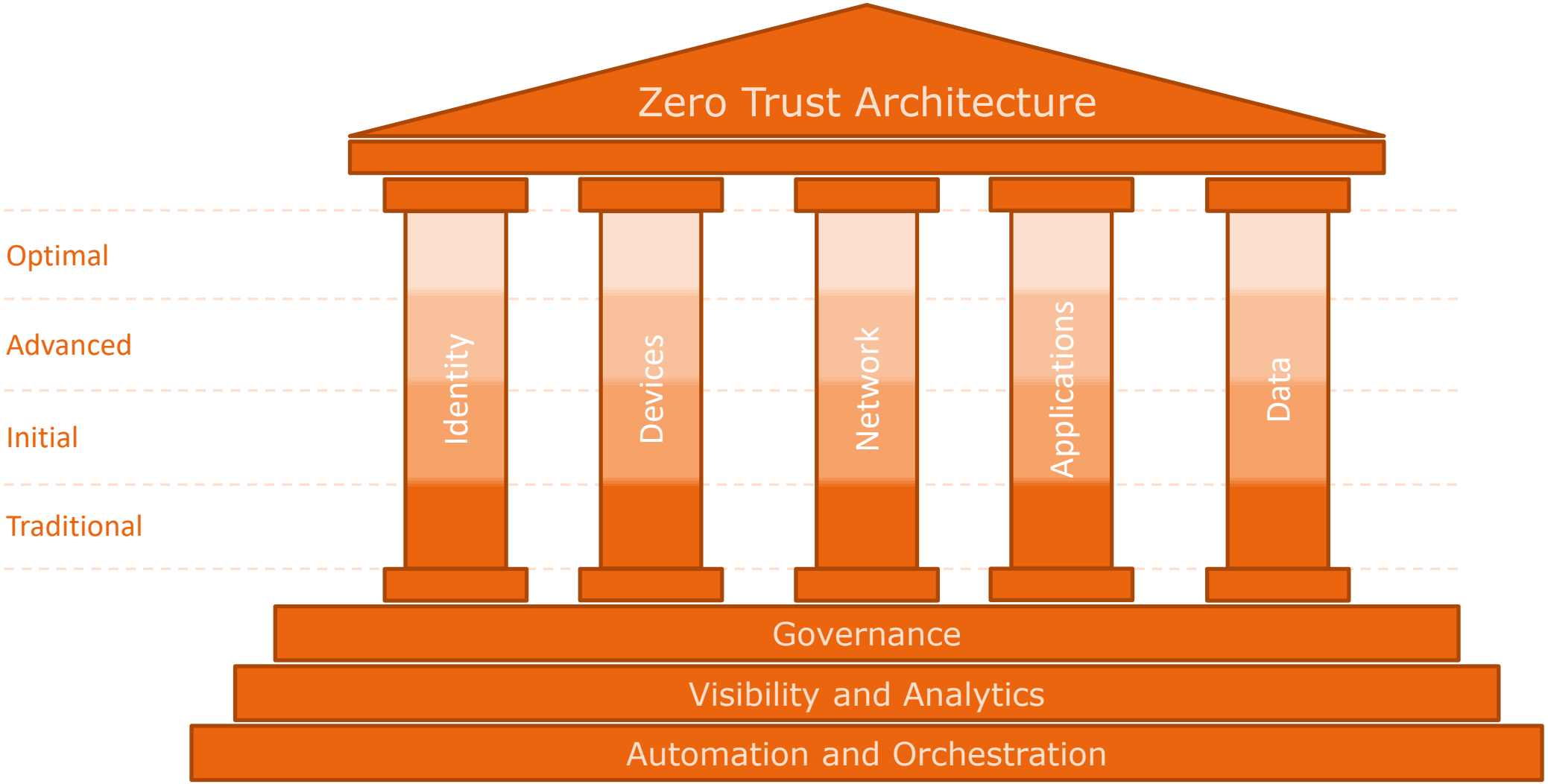


Karakteristieken:

- Geen agents vereist voor de afhandeling van toegang
- Er is minder informatie beschikbaar om het vertrouwensniveau te bepalen
- Potentieel single-point-of-failure en doelwit voor DDoS aanvallen
- Geschikt voor BYOD scenario's en voor samenwerking tussen organisaties

Bron: NIST 800-207

CISA Zero Trust Maturity Model

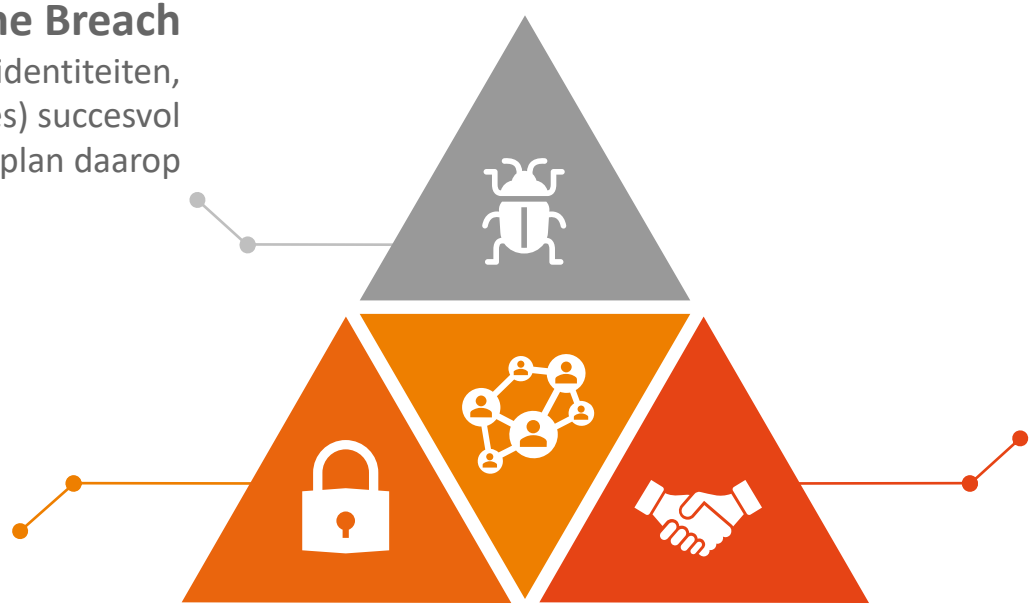


Bron: Cybersecurity & Infrastructure Security Agency

Conclusie Zero Trust Architectuur

Assume Breach

Ga ervan uit dat hackers alles (identiteiten, apparaten, netwerken, applicaties) succesvol kunnen aanvallen en plan daarop



Never Trust, Always Verify

Bescherm resources tegen hackers door alle relevante informatie die beschikbaar is mee te wegen in besluiten voor toegang

Use least-privilege access

Beperk toegang tot resources met minimale en just-in-time rechten, idealiter met dynamische toegangscontrole

NN

Zero Trust Aanpak

Het slechte nieuws

- Er is geen silver bullet.
- Er is namelijk geen product op de markt waarmee Zero Trust op magische wijze kan worden geïmplementeerd.

Goed nieuws!

- Je hebt waarschijnlijk al veel capabilities in huis die waardevol zijn in een Zero Trust architectuur!

Doe onderzoek

- Kijk naar NIST als je van theorie houdt en naar het CISA ZTMM als je wilt weten waar je staat.

Maak het plan

- Zero Trust is een reis. Ontwikkel de Zero Trust roadmap voor jouw organisatie en ga op pad!

Zero Trust bij NN Group

Zero Trust bij NN Group

- Uitgangspunten
- Oplossing
  - Componenten (Client, Service Edge , Gateway)
  - Resilience
  - Applicatie Segmentatie
- Projectaanpak en afstemming
- Lessons learned
- Aanbevelingen

Zero Trust – een aantal uitgangspunten

- er is geen ‘silver bullet’ oplossing die de Zero Trust Architecture volledig implementeert
- Zero Trust User Access is een technologie waarin Zero Trust principes worden toegepast
- users moeten hun public en private applications kunnen benaderen via een internet connectie
- oplossing moet voldoen aan NN security and compliancy policies en standaarden
- integratie met de huidige en toekomstige werkplek oplossingen
- Resilience, High availability, Disaster Recovery

Scope

- ~ 20.000 users
- end-point devices (Windows, MacBook, Mobiles)
- alle Business Units binnen NN Group

"Transition to Zero Trust is a journey"

Wijzigingen in de keten van gebruikers met verschillende devices verbinding maken via verschillende netwerken met NN Apps

Gebruikers

- "Working anywhere, anytime on any device"

Devices

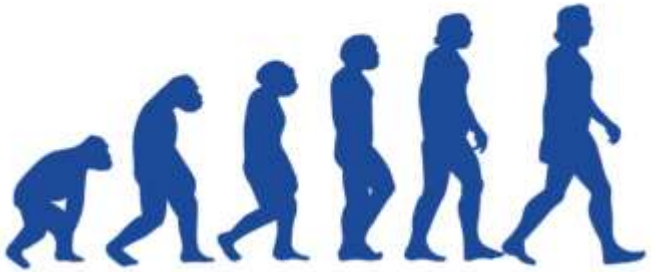
- Managed laptop, CYOD, BYOD, Mobile

Netwerken

- Remote Access, Cloud, WAN, OfficeLAN, Datacenter

NN Applicaties

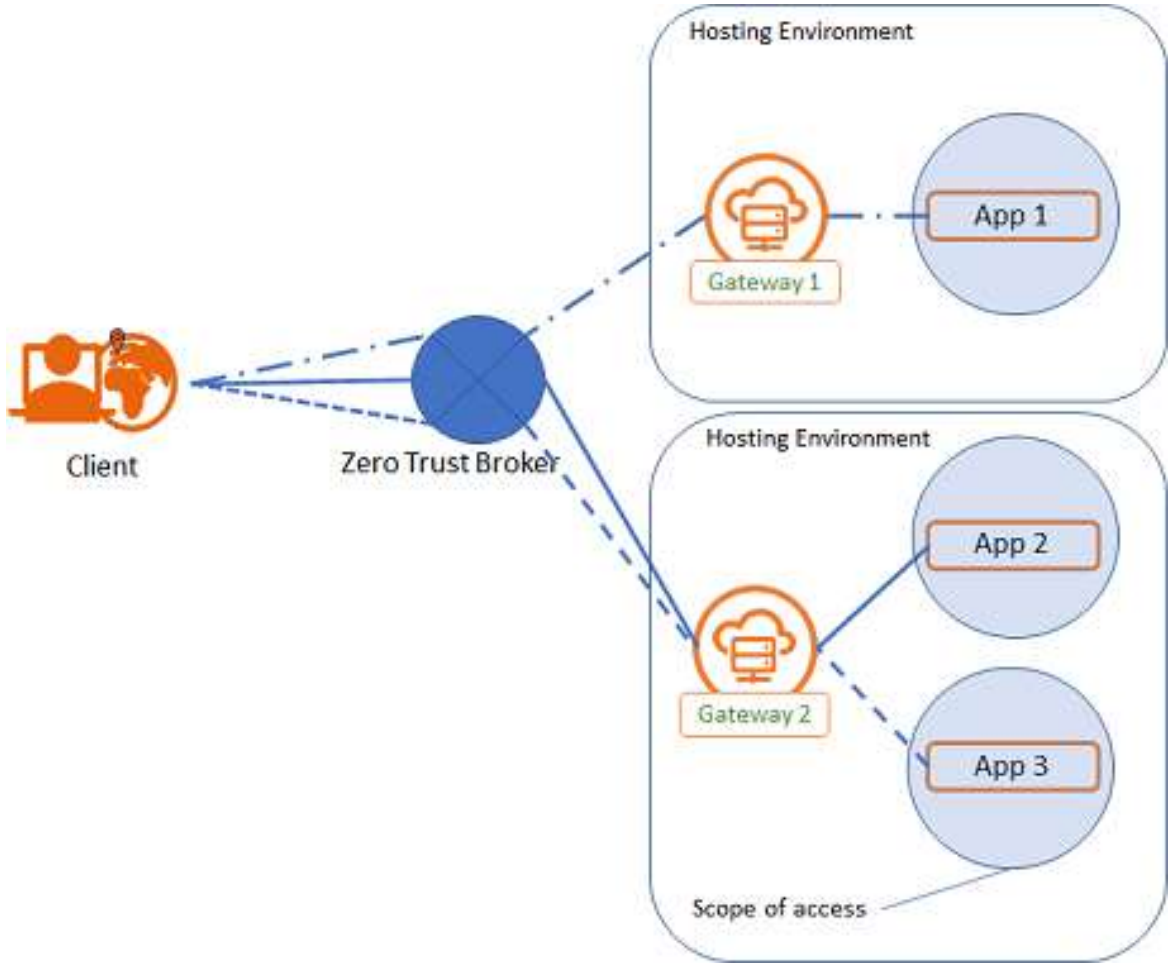
- Private on-prem apps, private cloud apps en internet apps



Fases: 1. Vervangen VPN → 2. Applicatie Segmentatie → 3. Conditional Access

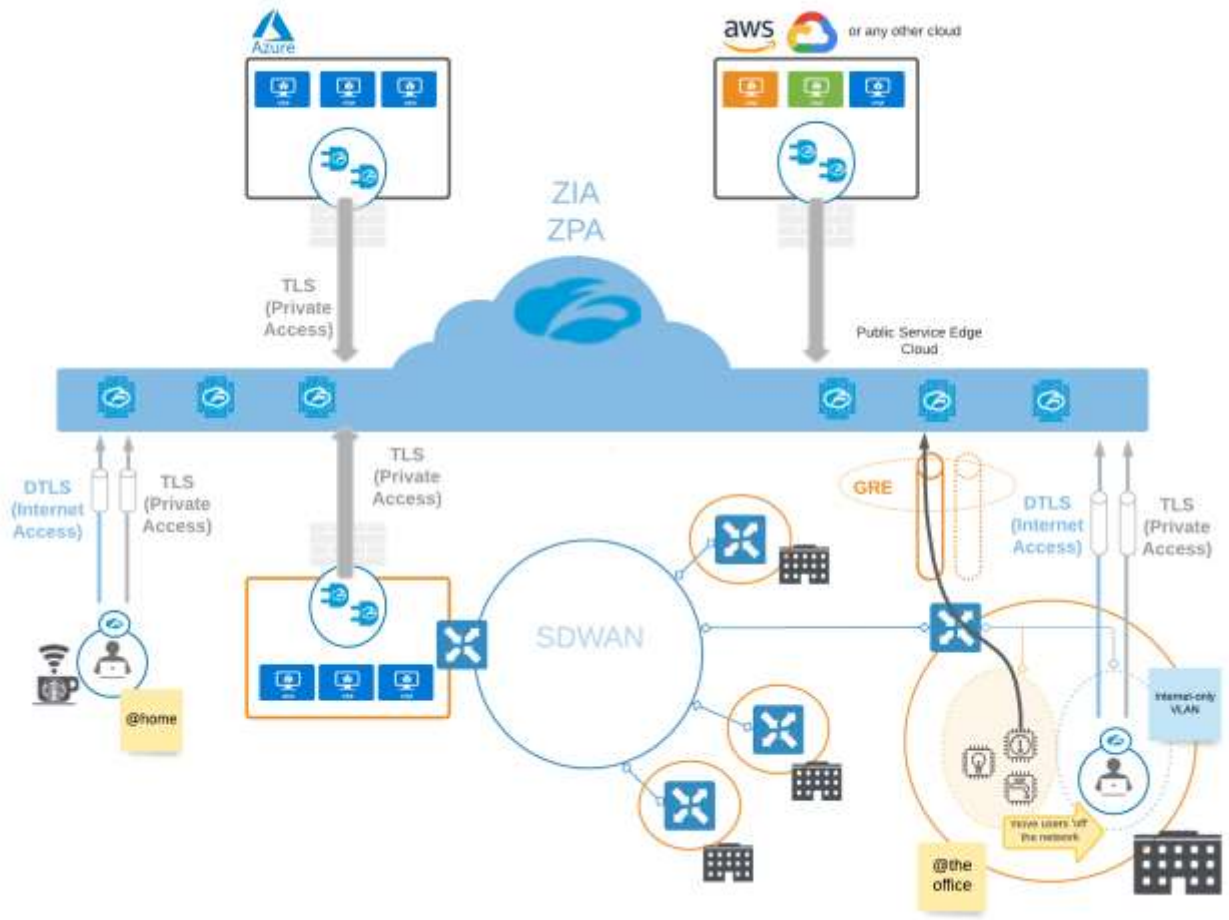
NN

Zero Trust User Access



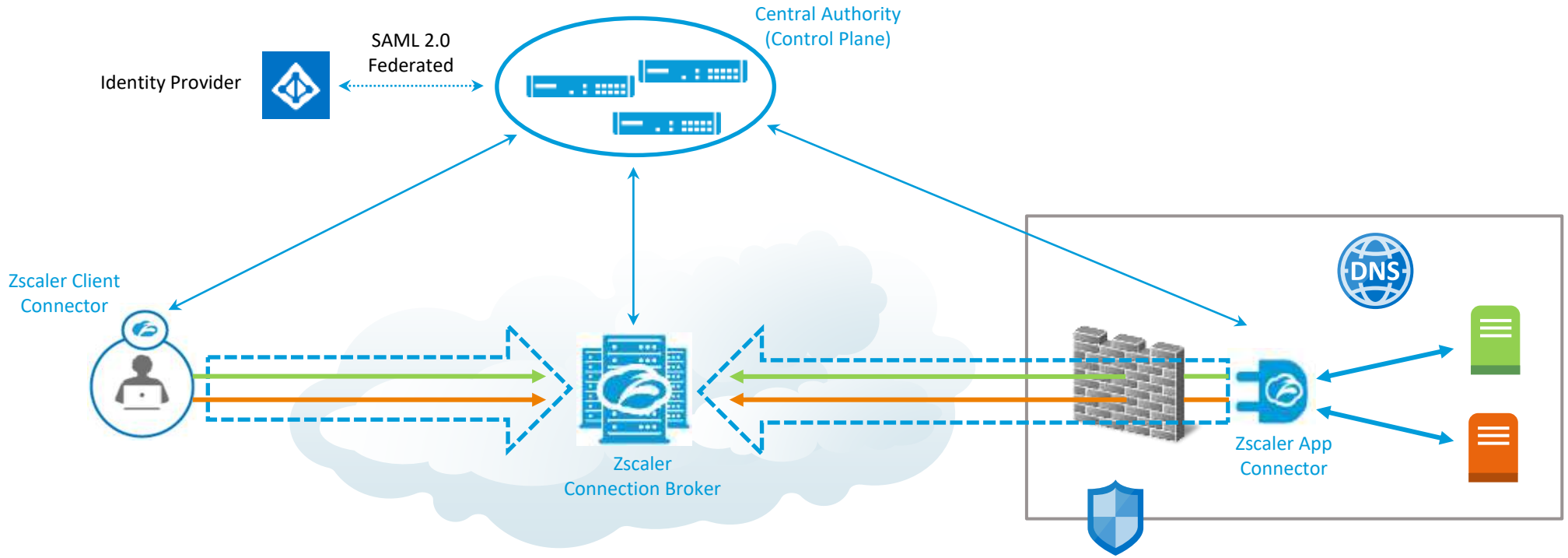
NN

Internet Access en Zero Trust User Access



NN

Zero Trust User Access



Resilience

 **Blackout** *Data center outage / Connectivity issues*	 **Brownout** *Hot cluster / Connectivity issues*	 **Catastrophic Failure** *Cloud outage / Connectivity issues*
Datacenter outage of connectivity issues	**Performance degradatie**	**Cloud outage of connectivity issues**
Automatische tunnel fail-over naar ander datacenter	Dynamische Service Edge selectie op basis van performance	Disaster Recovery door Private Service Edge
	Uitsluiten van datacenters	

Wat is een Zero Trust enabled end-user device?

Een Zero Trust enabled end-user device:

- is een supported laptop/desktop (Windows of Mac OS-X) of mobile device (iOS or Android)
- is enrolled met Intune met een multi-factor authenticated NN Group user credential
- heeft security policy enforced inclusief update regime en secure configuration
- heeft een Zero Trust Client Connector agent geïnstalleerd die een connectie biedt naar NN Group private applications

Een Zero Trust User Access enabled end-user device beveiligt:

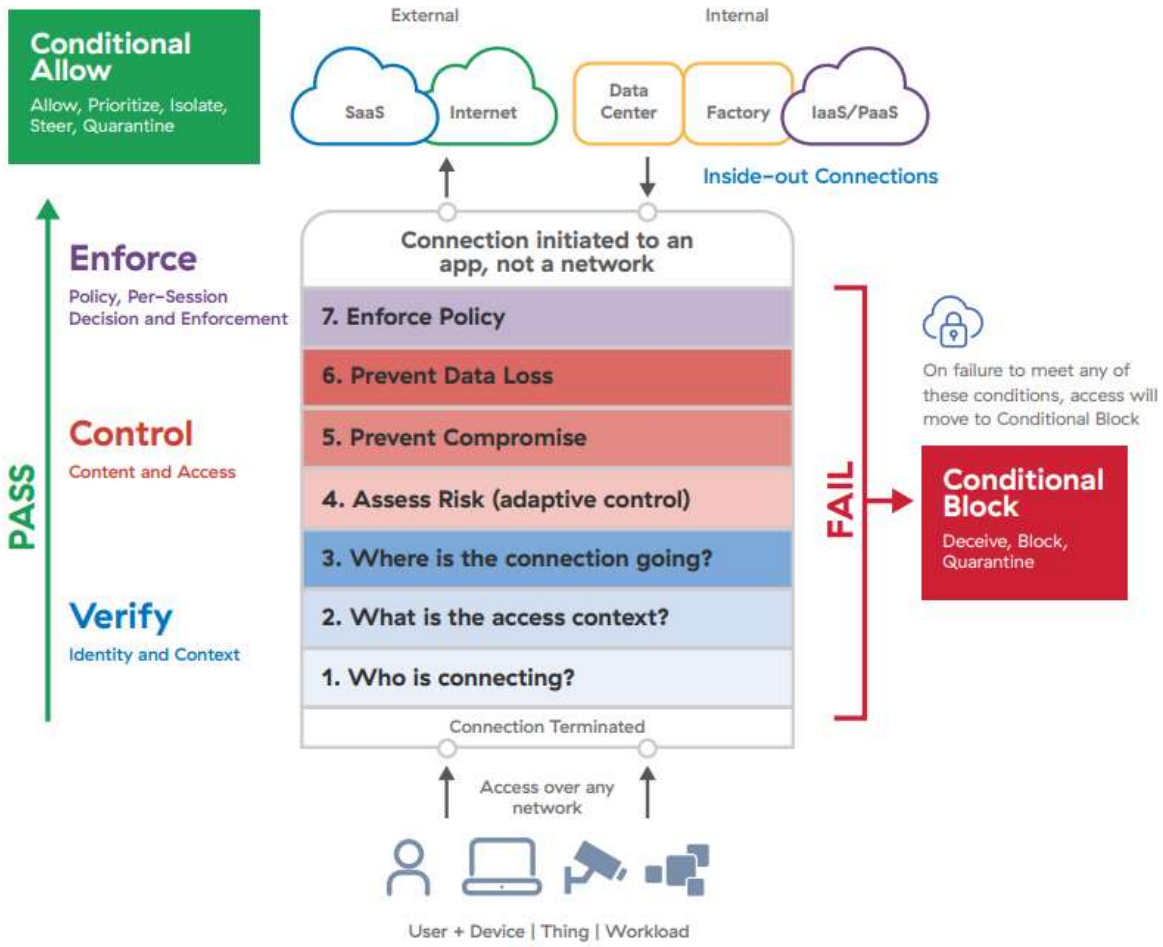
- internet verkeer met Zscaler Internet Access (ZIA)
- NN Group private application verkeer met Zscaler Private Access (ZPA)
- lokaal netwerkverkeer met een built-in firewall

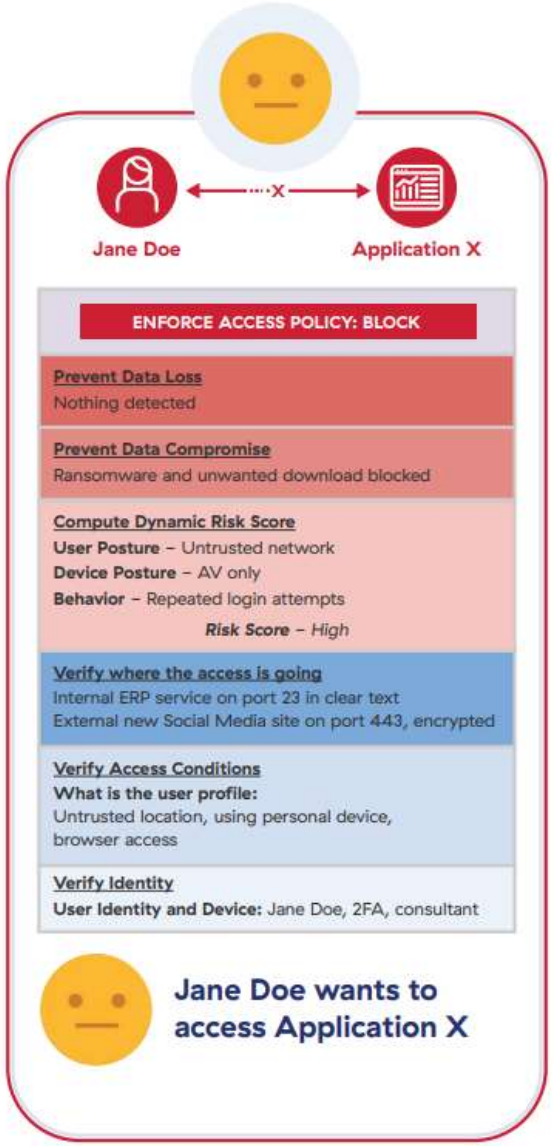
To deliver full functionality a zero-trust end-user device only requires internet connectivity (“McDonald’s model”)

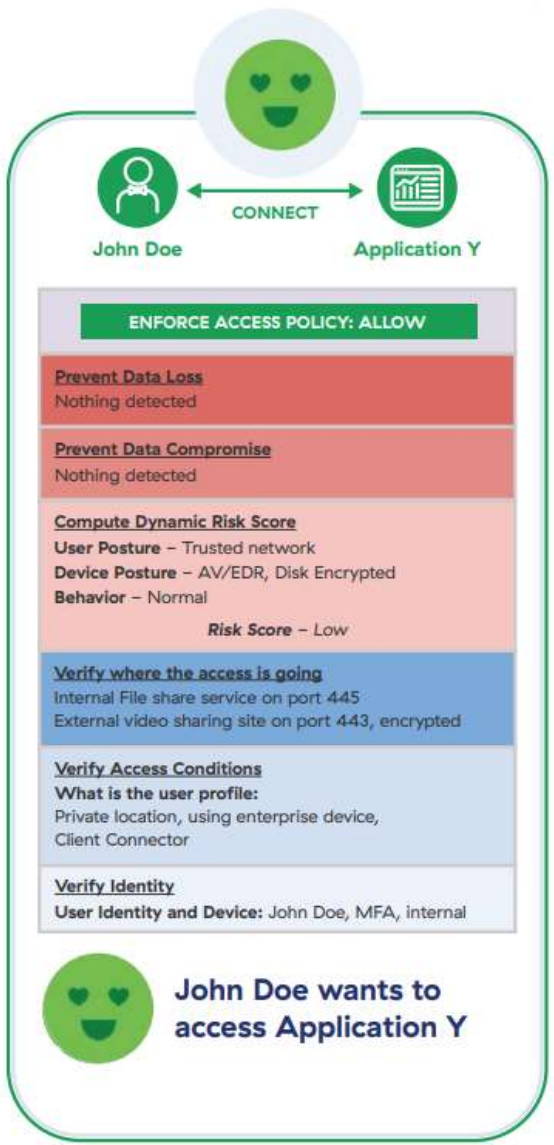
Still having a highway into the datacenter defeats the purpose of zero trust user access

NN

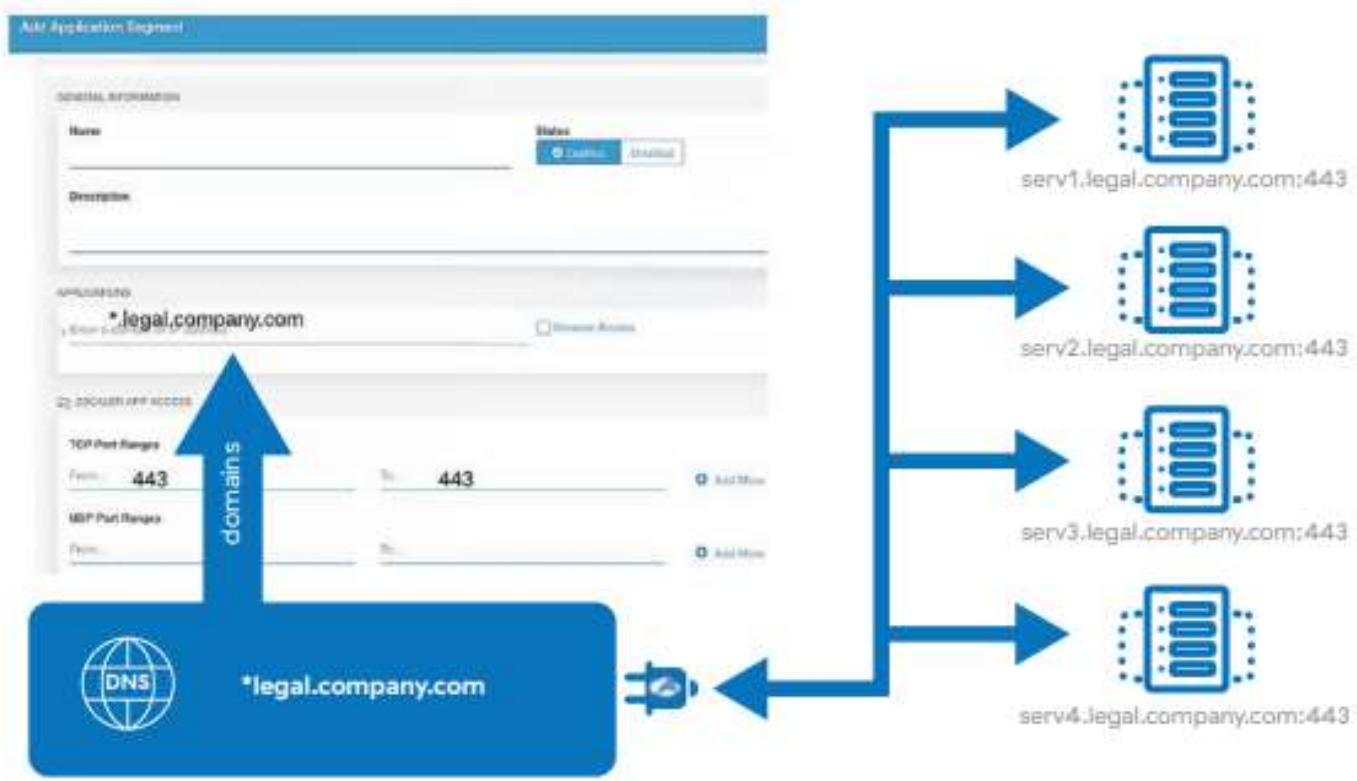
Zero Trust Architectuur



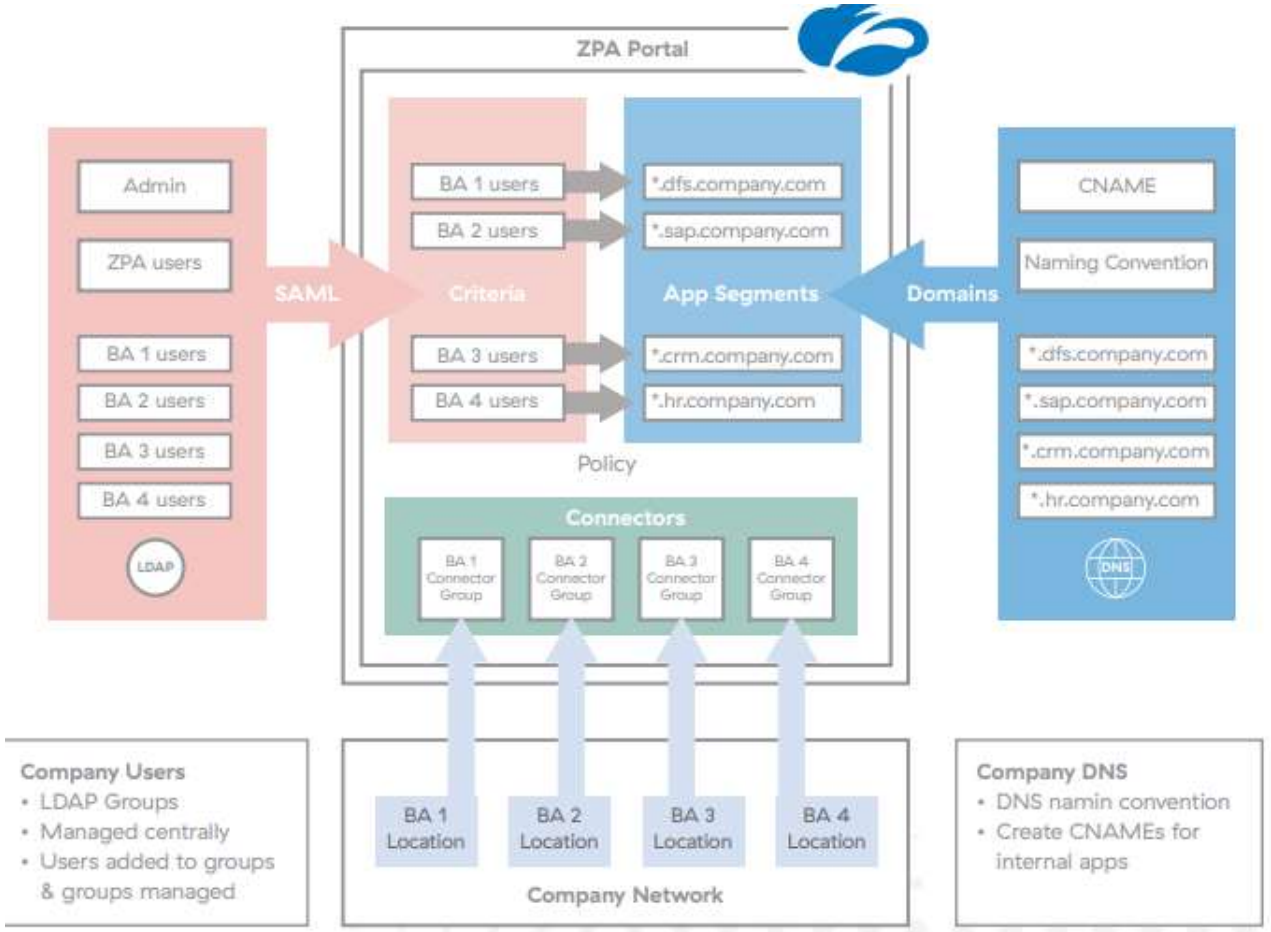

Jane Doe
X
Application X
ENFORCE ACCESS POLICY: BLOCK
Prevent Data Loss
Nothing detected
Prevent Data Compromise
Ransomware and unwanted download blocked
Compute Dynamic Risk Score
User Posture – Untrusted network
Device Posture – AV only
Behavior – Repeated login attempts
Risk Score – High
Verify where the access is going
Internal ERP service on port 23 in clear text
External new Social Media site on port 443, encrypted
Verify Access Conditions
What is the user profile:
Untrusted location, using personal device, browser access
Verify Identity
User Identity and Device: Jane Doe, 2FA, consultant
Jane Doe wants to access Application X


John Doe
CONNECT
Application Y
ENFORCE ACCESS POLICY: ALLOW
Prevent Data Loss
Nothing detected
Prevent Data Compromise
Nothing detected
Compute Dynamic Risk Score
User Posture – Trusted network
Device Posture – AV/EDR, Disk Encrypted
Behavior – Normal
Risk Score – Low
Verify where the access is going
Internal File share service on port 445
External video sharing site on port 443, encrypted
Verify Access Conditions
What is the user profile:
Private location, using enterprise device, Client Connector
Verify Identity
User Identity and Device: John Doe, MFA, internal
John Doe wants to access Application Y

Applicatie segmentatie



Applicatie segmentatie

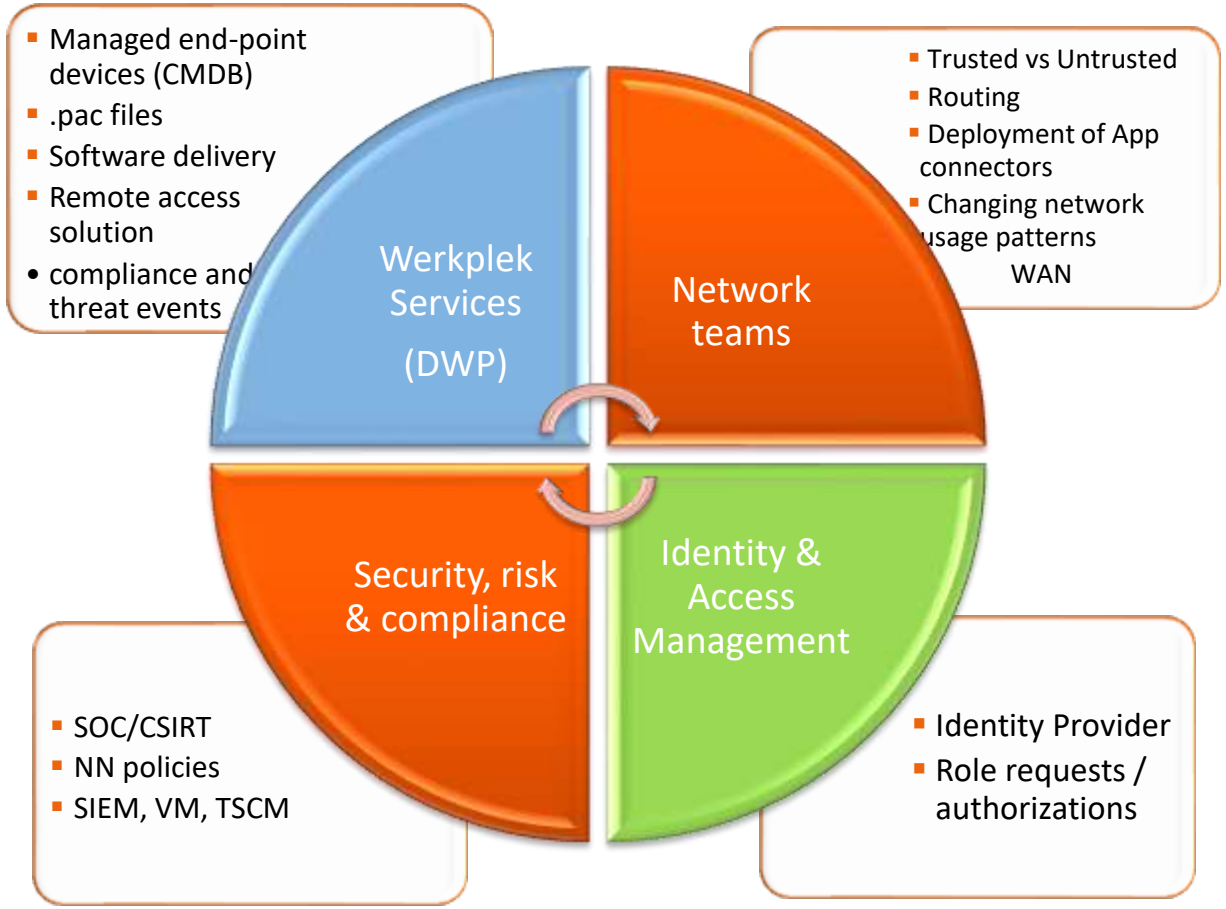


Zero Trust project aanpak

"Approach to adopting a Zero Trust User Access Architecture"

- bepaal de scope Zero Trust User Access
- bepaal functionele and non-functionele requirements inclusief migratie
- breng de afhankelijkheden, relaties en impact op andere technologie in kaart
- maak een Longlist van kandidaat ZTUA producten en assess
- maak een Shortlist van kandidaat ZTUA producten en execute PoC
- selecteer ZTUA product
- ontwerp en implement ZTUA infrastructuur
- pilot en 'eat your own dog's food’
- maak service design van ZTUA
- migreer clients naar ZTUA infrastructuur
- implementeer applicatie segmentatie

Afstemming met andere NN DevOps teams



IAM

- Unique identities and robust authentication service are required
- Consistent mapping of applications to access groups and authorized users to access groups
- Orchestration of application access groups to ZTA solution

NN

Lessons learned

- meer incidenten worden toegewezen aan ons team
- grote afhankelijkheid van Zscaler services en verstoringen hebben grote impact
- oplossing nodig voor “server initiated traffic” (remote support and telefonie)
- netwerk engineers en developers moeten wennen aan het nieuwe model
- Stepping stone nodig voor engineers
- LAN en WAN netwerken worden minder relevant
- connectivity naar gateways moet geregeld worden
- onboarden van applicaties is complex en tijdrovend
- technische issues

Aanbevelingen

- ontwikkelingen gaan erg snel en kijk goed naar de verschillende implementaties en Gartner kwadrant
- begin met ZTUA implementatie met een wildcard (VPN mode) en daarna applicatie segmentatie
- begin applicatie segmentatie met afdelingen of rollen
- voorkom verschillende ‘user experiences’ tussen locaties
- architectuur – “first time right with end-state in mind to reduce complexity”
- communiceer veel met stakeholders
- uitgebreide pilot
- zorg voor internet connecties
- nodig ons uit voor de koffie als je meer wilt weten van een ZTUA implementatie

Vervolgstappen

- afronden Zero Trust uitrol in de landen
- onboarden van applicaties voor Application Segmentation
- uitrollen gateways in Azure en AWS
- afstemmen Conditional Access met Application owners
- oplossing bepalen voor Virtuele werkplekken
- oplossing bepalen voor IoT
- oplossing bepalen voor Workloads

"Keep the data in and the hacker out"


Kom maar op
met die digitale toekomst


NN