QUANT ICT
Smart Network

Zeg vaarwel tegen VPN. Waarom Zero Trust de nieuwe standaard is

Hoe Zero Trust Network Access (ZTNA) en Secure Service Edge (SSE) klassieke VPN's vervangen: veiliger, eenvoudiger en klaar voor NIS2

HPE

Waarom VPN zijn beste tijd heeft gehad

Er was een tijd dat Virtual Private Network (VPN) dé standaard was voor veilige externe toegang. Wie niet op kantoor zat, gebruikte VPN om van-op afstand toegang te krijgen tot het bedrijfsnetwerk. In essentie creëerde een VPN een tunnel waardoor dataverkeer veilig naar binnen kon.

Vergelijk het met het kasteelmodel van de digitale werkplek. De gracht en de ophaalbrug (VPN + firewall) hielden jarenlang indringers buiten, terwijl medewerkers zich vrij binnen de muren konden bewegen. Vandaag volstaat die verdedigingslijn niet meer. Aanvallers geraken steeds gemakkelijker over, onder of zelfs dóór de kasteelmuren.

Tegelijk zijn de werkgewoonten in de huidige maatschappij sterk veranderd. Medewerkers werken niet alleen vanuit hun thuiskantoor, maar ook vanaf klantlocaties, coworkingruimtes, luchthavens en hotelkamers. De toepassingen die ze gebruiken staan vaak in de cloud, verspreid over de wereld.

Ook het aantal gebruikers van uw bedrijfsnetwerk is groter en diverser geworden. Niet alleen uw eigen medewerkers, maar ook leveranciers, onderaannemers, consultants en partners moeten toegang krijgen.

Klassieke VPN's zijn nooit ontworpen voor de huidige realiteit. Ze veroorzaken opstoppingen omdat al het verkeer via één poort moet. Eén enkele login opent te veel deuren, waardoor indringers zich vrij kunnen bewegen. En dat zorgt voor frustraties bij zowel de gebruikers als de IT-medewerkers.

De muren die ooit stevige bescherming boden, wankelen vandaag. Zodra iemand binnenraakt, ligt alles open. Geen verfijnde controle, geen continue check. In een wereld van ransomware en phishing is dat te risicovol. Zero Trust breekt met dit oude kasteelmodel: niemand krijgt nog blind vertrouwen, elke toegang wordt opnieuw streng gecontroleerd.

Wat is Zero Trust (en wat niet)?

Zero Trust is geen product dat u koopt en aansluit. Het is een beveiligingsfilosofie die het klassieke model omdraait. In het oude kasteelmodel was het doel om indringers buiten de muren te houden. Zero Trust gaat ervan uit dat dreigingen al binnen zijn.

Zero Trust gaat, zoals de naam het zelf al weggeeft, uit van nul vertrouwen. Concreet betekent dit dat elke gebruiker, elk apparaat en elke applicatie zich telkens opnieuw moet authenticeren. En zelfs dan krijgen ze enkel toegang tot wat strikt noodzakelijk is, en niets meer.

Als we het kasteelmodel doortrekken, dan installeert Zero Trust meerdere controleposten binnen de muren: elke deur krijgt een badgelezer, elke gang een bewaker. Worden inloggegevens gestolen? Dan geeft dat hooguit toegang tot één kleine, bewaakte ruimte. Zero Trust is dus een mindset. Het gaat niet langer om het bouwen van een vaste barrière en hopen dat die standhoudt. Voortaan wordt elke interactie – hoe klein ook – gecontroleerd. Continu, zonder uitzondering.

Hoe past Zero Trust in het NIS2-verhaal?

NIS2 is de nieuwe Europese richtlijn voor netwerk- en informatiebeveiliging. Ze verplicht organisaties in essentiële en belangrijke sectoren, zoals energie, zorg, transport, financiën, digitale diensten en de publieke sector, om hun beveiliging tegen cyber threats aanzienlijk te versterken.

Voor veel organisaties betekent dit dat klassieke VPN-oplossingen tekortschieten. NIS2 vraagt precies de capaciteiten die Zero Trust biedt: fijnmazige toegangsrechten, permanente verificatie en volledige zichtbaarheid.
In de praktijk gaat het om:

- **Volledige zichtbaarheid:** weten wie toegang heeft tot wat, en alle activiteiten loggen.
- **Least privilege:** enkel de strikt noodzakelijke rechten toekennen.
- **Continue monitoring:** verdachte activiteiten detecteren en compliance kunnen aantonen.

ZTNA, SSE en SASE in gewone taal

Zero Trust is het principe. Om het in de praktijk te brengen zijn technologieën nodig die dit afdwingen.

ZTNA – Zero Trust Network Access

ZTNA is de eerste, tastbare laag van Zero Trust. In plaats van verbinding met het hele netwerk geeft ZTNA alleen toegang tot de specifieke dienst of applicatie die u nodig hebt. Bent u een leverancier die in het besturingspakket van een machine moet ingrijpen, dan geeft ZTNA enkel toegang tot dat specifiek besturingspakket. Gebruiker én apparaat worden geauthenticeerd, hun beveiligingsstatus gecontroleerd en vervolgens via een versleutelde verbinding rechtstreeks gekoppeld aan de juiste resource. Het bredere netwerk blijft onzichtbaar.

SSE – Secure Service Edge

SSE is de cloudgebaseerde beveiligingslaag, die onder meer het volgende omvat:

- **ZTNA** voor beveiligde toegang tot een (of meerdere) applicaties.
- **Secure Web Gateway (SWG)** om het webverkeer te filteren en zo malafide websites, phishing-pogingen en gevaarlijke downloads te blokkeren.
- **Cloud Access Security Broker (CASB)** monitort en beveiligt het gebruik van cloudapps (Microsoft 365, Salesforce, enz.).
- **Data Loss Prevention (DLP)** om datalekken (persoonsgegevens, bedrijfsgeheimen, enz.) te voorkomen.

SSE zorgt voor bescherming van de gebruikers, waar ze ook werken, en bieden systeembeheerders volledige zichtbaarheid.

SASE – Secure Access Service Edge

SASE combineert SSE met SD-WAN (software-defined WAN). Deze technologie verzekert dat de beveiliging de gebruiker volgt: zij is niet gebonden aan kantoor, firewall of VPN-gateway.
Naast beveiliging optimaliseert SASE de prestaties van netwerkverbindingen tussen vestigingen, datacenters en clouddiensten.

Waarom switchen van VPN naar Zero Trust?

De 6 grootste voordelen

1. Sterkere beveiliging

Met VPN krijgt een gebruiker na één login vaak toegang tot veel meer systemen dan nodig. Bij misbruik kan een aanvaller zich vrij door het netwerk bewegen.

Met Zero Trust wordt toegang beperkt tot één specifieke applicatie, continu opnieuw geverifieerd en gelogd.

➔ **Resultaat:** indringers raken nooit verder dan het strikt noodzakelijke.

2. Altijd en overal toegang

VPN vraagt telkens om manueel te verbinden en vertraagt omdat al het verkeer via een centrale gateway loopt.

ZTNA/SSE maakt verbindingen transparant en stuurt verkeer rechtstreeks naar de juiste (cloud) applicatie.

➔ **Resultaat:** gebruikers werken overal veilig én vlot.

3. Eenvoudiger beheer

VPN-landschappen bestaan vaak uit verschillende clients, versies en configuraties die tijd en fouten kosten.

ZTNA/SSE centraliseert toegangsbeheer in één cloudplatform en voert beleidswijzigingen meteen door, zonder endpoints te herconfigureren.

➔ **Resultaat:** minder complexiteit en minder operationele druk op IT.

4. Veilige toegang voor derden

Via VPN krijgen leveranciers of partners al snel te brede rechten.
Met ZTNA loggen zij in via een beveiligd webportaal en zien ze enkel wat relevant is. Dit is extra handig voor kortdurende projecten: u verleent en trekt toegang direct weer in.

➔ **Resultaat:** veilige toegang voor derden, zonder extra software of risico's.

5. Volledig zicht en controle

VPN laat alleen zien wie verbonden is en hoe lang.

ZTNA/SSE registreert welke applicaties zijn gebruikt, welke acties zijn uitgevoerd en vanaf welke locatie.

➔ **Resultaat:** realtime detectie van verdachte activiteiten, zodat u tijdig kan ingrijpen voor gevoelige data kan lekken, en eenvoudiger compliance met onder andere NIS2.

6. Toekomstbestendig en compliant

Het dreigingslandschap en de regelgeving evolueren constant.

ZTNA/SSE biedt ingebouwde dataminimalisatie, DLP en eenvoudige rapportage.

➔ **Resultaat:** klaar voor de uitdagingen van morgen en aantoonbaar compliant.

Sectoren waar Zero Trust het verschil maakt

Zero Trust, SSE en SASE zijn geen niches. Ze spelen in op uitdagingen van heel wat organisaties. Vooral in sectoren die onder NIS2 vallen, zijn de gevolgen groot: een inbraak kan leiden tot boetes, reputatieschade en kostbare stilstand.
Drie voorbeelden waar Zero Trust het verschil maakt:

Zorg

Met Zero Trust krijgt een huisarts enkel toegang tot de noodzakelijke dossiers, rechtstreeks en veilig vanuit de eigen praktijk. Het resultaat: patiëntgegevens blijven beschermd en de organisatie voldoet aantoonbaar aan NIS2.

Industrie

Productieomgevingen vormen aantrekkelijke doelwitten voor cyberaanvallen. Dankzij Zero Trust kan een technicus in het buitenland veilig toegang krijgen tot het specifieke controlesysteem van een productielijn, zonder bij de rest van het fabrieksnetwerk te kunnen.

Publieke sector & onderwijs

Deze sectoren werken met veel gebruikers en externe partijen, vaak verspreid over verschillende locaties. Met Zero Trust kunnen de netwerkbeheerders precies bepalen welke applicaties en gegevens voor deze gebruikers toegankelijk zijn en elke actie loggen. Bijgevolg kunnen alle gebruikers veilig verbinden en samenwerken vanaf elke locatie.

Hoe begint u met Zero Trust

De overstap naar Zero Trust hoeft geen sprong in het diepe te zijn. Succesvolle trajecten starten klein, tonen snel waarde en schalen daarna verder op.
Zes stappen voor een vlotte start:

1. **Focus op de grootste risico's:** start bij systemen of data waarvan verlies de meeste schade zou toedienen.
2. **Breng toegangsbehoeften in kaart**: bepaal precies wie wat nodig heeft. Zo ontdekt u snel ongebruikte accounts of te brede rechten die u direct kunt afsluiten.
3. **Start een pilot:** begin met een kleine groep en verfijn het beleid en de processen op basis van hun feedback.
4. **Houd het gebruiksvriendelijk:** integreer SSO en MFA zodat de beveiliging de gebruikers niet vertraagt.
5. **Monitor en verbeter:** gebruik de zichtbaarheid van het platform om afwijkingen tijdig te detecteren en regels bij te sturen.
6. **Breid stapsgewijs uit:** zodra de pilot stabiel is, rolt u verder uit naar andere teams, locaties en partners.

Onthoud: Zero Trust is geen eenmalig project. Elke stap verkleint uw aanvalsoppervlak, vergroot uw veerkracht en versterkt uw compliance, terwijl uw organisatie gewoon blijft draaien.

Waarom Quant ICT
als partner?

Zero Trust draait om expertise én technologie. Quant ICT levert:

- **Leveranciersonafhankelijkheid:** integratie van ZTNA/SSE in heterogene omgevingen.
- **Vlotte adoptie:** koppeling met bestaande systemen zoals Azure AD en Microsoft MFA.
- **Bewezen technologie:** HPE Aruba Networking als betrouwbare basis.
- **Doorlopende service:** monitoring, updates en support via Quant-as-a-Service.

“We don’t just implement and leave. We stay, we monitor, we adapt, because threats and needs change.”

Moet u uw VPN vervangen?

VPN is niet gebouwd voor de huidige realiteit. Vandaag creëert het vertragingen, blinde vlekken en complianceproblemen. ZTNA en SSE vormen de nieuwe standaard. Ze brengen:

- **Sterkere beveiliging.**
- **Eenvoudiger IT-beheer.**
- **Een betere gebruikservaring.**
- **Volledige zichtbaarheid.**

Met Quant ICT evolueert u in uw eigen tempo naar Zero Trust: klein beginnen, slim groeien en dreigingen altijd een stap voorblijven.

QUANT ICT
Smart Network

QUANT ICT
Industrieweg 4 bus 5
3001 – Heverlee

www.quant.be
+ 32 16 380 840
info@quant.be