

# Private Access

**Schakel snel, eenvoudig en veilig Zero Trust Network Access in op elke zakelijke bron.**

Geef teams de flexibiliteit om op elk moment en overal te werken door ze veilig te verbinden met de applicaties die ze nodig hebben. Private Access gebruikt identiteits- en app-gerichte beleidsregels om productiviteit mogelijk te maken en tegelijkertijd de brede vindbaarheid en bereikbaarheid van data en apps waartoe gebruikers geen toegang zouden mogen hebben, te elimineren.

## Sterke beveiliging

Private Access is ontworpen met een cloudgebaseerde software-gedefinieerde perimeter (SDP) die voor elke applicatie veilige, geïsoleerde verbindingen creëert. Door 'least-privilege'-handhaving en realtime controles van devices krijgen alleen specifieke, geautoriseerde gebruikers toegang tot applicaties. Microtunnels voor applicaties houden elke sessie apart en ingeperkt om zijdelingse verplaatsing te voorkomen.

## Verbeterde beheersbaarheid

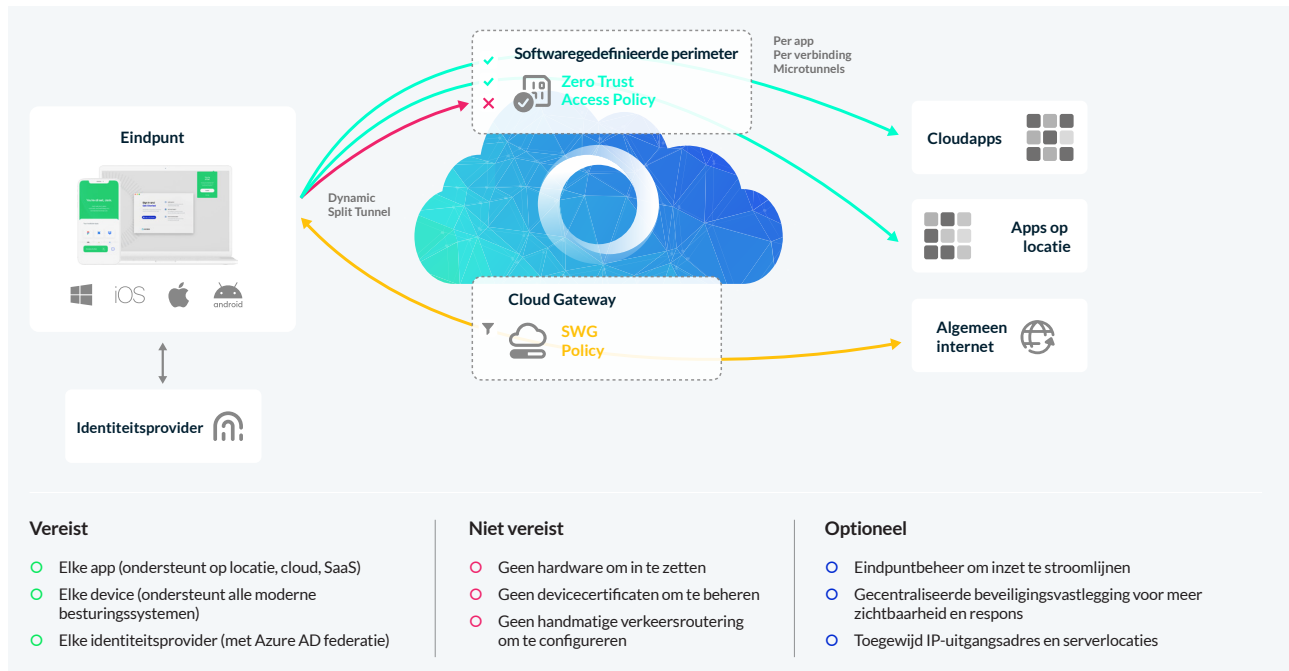
Private Access maakt gebruik van een volledig cloudgebaseerde architectuur, zodat het niet nodig is om devices op locatie te beheren en waarvoor geen complexe dimensioneringseisen gelden. Onze service is dynamisch uit te breiden om onbeperkte eindpuntverbindingen aan te kunnen. Private Access is efficiënter, omdat niet al het verkeer volledig hoeft te worden getunneld, wat onnodig duur is, maar zonder het zicht op en de controle over wat toegankelijk is, te verliezen (d.w.z. beleid zonder routing).

## Intuïtieve gebruikerservaring

Private Access maakt gebruik van een protocol dat speciaal is ontwikkeld om snel en veilig op afstand te werken. In combinatie met onze schaalbaarheid in de cloud en de mogelijkheid om onnodige backhauling van verkeer te vermijden, genieten gebruikers van een naadloze toegangservaring waarbij vertragingproblemen worden geëlimineerd. De service is efficiënt en past zich naadloos aan netwerkovertgangen aan, zodat de gebruiker ongestoord van mobiel netwerk naar wifi en weer terug kan gaan.

# Architectuur

Onze geavanceerde architectuur is gebouwd in de cloud en kan worden opgeschaald om elke applicatie die zowel in de cloud als op locatie wordt gehost, toegang te bieden.



## Kenmerken

### Cloud SDP

Private Access is ontwikkeld met een cloudgebaseerde softwaregedefinieerde perimeter die voor elke applicatie veilige, geïsoleerde verbindingen creëert. Door middel van 'least-privilege'-handhaving en realtime controles van devices, krijgen alleen specifieke, geautoriseerde gebruikers toegang tot elke applicatie.

### App-microtunnels

Private Access is een Zero Trust Network Access-oplossing waarbij het device en alle apps die erop worden uitgevoerd, blind zijn voor de netwerkinfrastructuur. Private Access maakt gebruik van microtunnels op app-niveau die door onze infrastructuur lopen, waardoor gedetailleerde controle mogelijk is, zowel bij het tot stand brengen van de verbinding als tijdens actieve sessies.

### Sessieverslaggeving

Dankzij gedetailleerde sessierapportages kunnen actieve gebruikers en de applicatie die zij gebruiken worden gemonitord. Realtime statistieken geven inzicht in ongebruikelijke activiteit, sessieduur of bandbreedtevereisten. Met de uitgebreide zichtbaarheid kunnen beheerders met een audit trail onpaste content controleren, malware opsporen en datalekken identificeren.

### Volgende-generatie protocollen

De meeste eindpunten gebruiken wifi of mobiele netwerkverbindingen, maar gebruikers en applicaties vereisen de prestaties die van een bekabelde verbinding worden verwacht. Private Access maakt veilig verbinden snel, veelzijdig en licht, door een stille en naadloze service te bieden, zelfs voor de gebruiker die onderweg werkt.

### Oplossing op basis van identiteit

Private Access gebruikt beleidsregels op basis van identiteit om gebruikers- en toepassingsmachtigingen toe te wijzen. Door bestaande directorydiensten te integreren is een snelle inzet en beheer van beleidslijnen mogelijk. De enige manier om een tunnel tot stand te brengen is dat de gebruiker de juiste rechten heeft voor de gespecificeerde toepassing.

### Dynamische split-tunnel

Private Access maakt gebruik van een intelligent tunneling-protocol dat alleen het verkeer van een applicatie op het device van de geautoriseerde gebruiker routeert naar de bijbehorende applicatie aan de andere kant van de Cloud-SDP. Dit zorgt ervoor dat het microtunnelbeleid van de applicatie goed wordt gehandhaafd, terwijl de eindgebruiker een optimale ervaring krijgt, omdat er geen onnodig verkeer door de beveiligde applicatietunnel stroomt.

### Single Packet Authorization

Elimineer de detecteerbaarheid van applicaties door niet-geverifieerde partijen. Single Packet Authorization vereist dat de identiteit van de gebruiker en het device wordt geverifieerd voordat toegang wordt verkregen. Dit betekent dat alleen verbindingsoogingen van geautoriseerde gebruikers worden herkend, waardoor uw services 'donker' lijken voor alle anderen op het internet.

### Adaptieve toegang

Private Access biedt realtime risicobeoordelingen van gebruikers en devices die routes kunnen beïnvloeden en als signalen kunnen worden gebruikt via integraties van derden. Als de risicostatus van een device verandert, kan Private Access in realtime een sessie beëindigen of routes wijzigen, in overeenstemming met het beleid.