eurofiber

Betere zorg door de cloud

Wat is de ideale verbinding voor de toekomst?

LIFELINE

Cloud-watervrees? Dat is echt niet nodig

Zowel onze samenleving, als specifiek de zorgbranche veranderen door de komst van Internet of Things, robotisering, kunstmatige intelligentie en sensoring. We zitten midden in Industry 4.0: een revolutie waarin computers en automatisering samenkomen en voor grote veranderingen zorgt.

Zo geeft deze revolutie zorgprofessionals bijvoorbeeld zeer bruikbare tools in handen. Denk maar eens aan de mogelijkheden van big data waarmee je geneeskundige verbanden ontdekt. Of e-health oplossingen voor metingen op locatie. Het zijn tools die bijdragen aan snellere diagnoses en effectievere behandelingen.

Connectiviteit van vitaal belang

Industry 4.0 draait om data. Om toegang tot deze data te krijgen is connectiviteit cruciaal. Wat u ziet is dat ook in de zorgbranche mensen, platformen, netwerken, apparaten en systemen steeds meer met elkaar verbonden raken.

Dat levert prachtige kansen op, maar ook veel bedreigingen. We worden immers steeds meer afhankelijk van ICT en communicatie. Ligt dat stil, dan ligt de zorgbranche ook stil.

Optimalisatie

In industry 4.0 staat naast innovatie ook kostenbesparing centraal. Bijvoorbeeld door ondersteunende en administratieve processen te optimaliseren. Dit is essentieel bij onze vergrijzende samenleving waarbij kwalitatieve zorg betaalbaar moet blijven.

De cloud biedt kansen in de zorg

Voor uw organisatie is het van groot belang in te spelen op alle veranderingen. Maar hoe doet u dit? Hoe maakt u uw organisatie flexibel en wendbaar? De cloud maakt het gemakkelijker en laagdrempeliger om met uw organisatie te versnellen en te experimenteren. In dit e-book nemen we u mee in deze nieuwe wereld. Wat zijn de voordelen voor uw organisatie en waarom is beveiliging nog belangrijker dan in ons traditionele IT-landschap? Ontdek de mogelijkheden van de cloud en hoe u veilig en direct toegang krijgt tot meerdere cloud platformen.

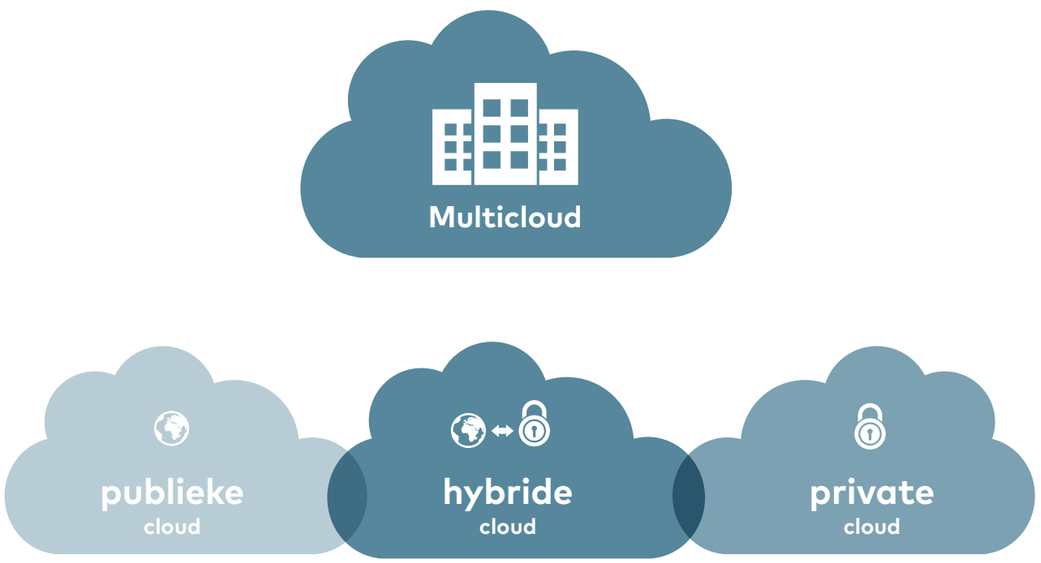
Inhoud

1. Welke cloud vorm past bij uw organisatie?

Welke keuzes zijn er allemaal?

De behoefte in de zorgbranche om snel in te spelen op veranderingen en het terugdringen van kosten zijn belangrijke argumenten om uw cloud strategie onder de loep te blijven nemen. U maakt continue keuzes om tot een optimale cloud omgeving te komen. Kiest u daarbij voor een publieke, private, hybride of multicloud?

Vanwege de verschillende eisen van organisaties, zijn er ook verschillende gebruikers-modellen: publieke, private en hybride cloud. Maar ook multicloud strategie behoort tot de mogelijkheden. Kies de vorm die het best voldoet aan de eisen van uw organisatie.



Welk model past bij uw organisatie?

Private cloud

Wanneer we de gevirtualiseerde IT-omgeving uitsluitend voor het eigen bedrijf gebruiken, dan spreken we van een private cloud. Bij private cloud staan de applicaties en diensten bij de cloud provider in een beheerd datacenter of in het eigen datacenter, net als bij de publieke cloud. Echter, een private cloud is een volledig afschermde IT-omgeving met eigen servers voor applicaties en gegevensopslag. Uw eigen IT-afdeling zorgt voor het beheer en onderhoud (of desgewenst een speciaal team van de cloud provider).

Voordelen

- Op maat gemaakt. De applicaties en diensten zijn afgestemd op de behoeften van uw organisatie.
- Privacy overweging. U weet altijd exact waar uw data is opgeslagen. Voor bijvoorbeeld zorginstellingen is dat van cruciaal belang; de wet- en regelgeving eist dat zij precies weten waar de gegevens staan én hoe de beveiliging is geregeld.

Nadelen

- Hogere investeringen. Door het maatwerk dat bij een private cloud komt kijken, is deze oplossing mogelijk duurder dan de publieke cloud. Denk aan extra investeringen voor hardware, fysieke beveiliging en continuïteit. Ook moet er rekening gehouden worden met hogere kosten voor het opschalen van extra capaciteit.

Publieke cloud

De naam zegt het al: de publieke cloud is voor iedereen toegankelijk. Deze cloud bestaat uit een gevirtualiseerde IT-omgeving waarbij verschillende organisaties elk een eigen IT-omgeving, inclusief besturingssysteem, gebruiken. De cloud provider werkt met een aantal standaard configuraties voor netwerkservers, cybersecurity, applicaties en gegevensopslag. Het beheer en onderhoud van de IT is voor rekening van de cloud provider.

Voordelen

- Relatief lage investering. Door de standaard configuraties kan de cloud provider een behoorlijk aantal klanten bedienen. Wat zorgt voor een relatief lage prijsstelling.
- Snel doorvoeren van nieuwe ontwikkelingen. De publieke platformen hebben de capaciteit om nieuwe ontwikkelingen snel te implementeren.
- Schaalbaarheid. Voor tijdelijke projecten kunt u snel extra opslagruimte of rekenkracht inzetten.
- Cloud providers hebben vaak een hoge volwassenheid op het gebied van informatiebeveiliging. Denk aan maatregelen op het vlak van fysieke beveiliging, toegangscontrole, gegevensopslag en continue training van gespecialiseerd personeel.

Nadelen

- Beperkte mogelijkheden voor maatwerk. Er is een groot aanbod aan applicaties en diensten beschikbaar, maar deze moeten maar net helemaal aansluiten bij de specifieke IT-behoeften van uw organisatie.
- Privacy overwegingen. Bij de publieke cloud is het niet inzichtelijk op welke systemen en in welke landen de gegevens zich bevinden. Soms eist de overheid van organisaties dat zij bepaalde gegevens altijd in eigen beheer houden.

Hybride cloud

De hybride cloud is een combinatie van de publieke en private cloud. De hybride cloud biedt u kortgezegd 'best of both worlds'. Zo gebruikt u het standaard aanbod van de publieke cloud, zoals Microsoft Azure, Amazon Web Services of Google Cloud Platform.

Daarnaast maakt u gebruik van maatwerkoplossingen om aan privacy-wetgeving te voldoen of om eigen sector- of bedrijfsspecifieke software te blijven toepassen. Deze handige combinatie zorgt ervoor dat de hybride cloud steeds populairder wordt.

"Eurofiber biedt een totaaloplossing waarbij de complete cloud strategie wordt ingeregeld"

Voordelen

- Financieel aantrekkelijke standaard configuraties met de snelheid en flexibiliteit van de publieke cloud.
- Maatwerkoplossingen voor specifieke applicaties en systemen zoals in de private cloud.

Nadelen

- Hogere investeringen dan voor de publieke cloud.
- Complexiteit van het combineren van de publieke en private cloud.

Multicloud

Multicloud houdt in dat u meerdere clouddiensten van verschillende providers gebruikt. Reden voor deze aanpak of strategie is dat u optimaal flexibel bent in uw keuze. Heel specifieke workloads (functionaliteiten) vereisen vaak elk een eigen clouddienst afkomstig van verschillende cloud providers.

Het grootste verschil met de hybride cloud is dat multicloud echt een strategie is en de hybride cloud een technische oplossing. De hybride cloud houdt in dat u van zowel een publieke als private cloud (zowel managed als on-premise/in huis) gebruik maakt, om de workload te verdelen over de juiste omgeving, op het juiste moment.

Hoewel de termen dus totaal iets anders betekenen, ligt aan beide wel een flexibele strategie ten grondslag.

"Optimale flexibiliteit"

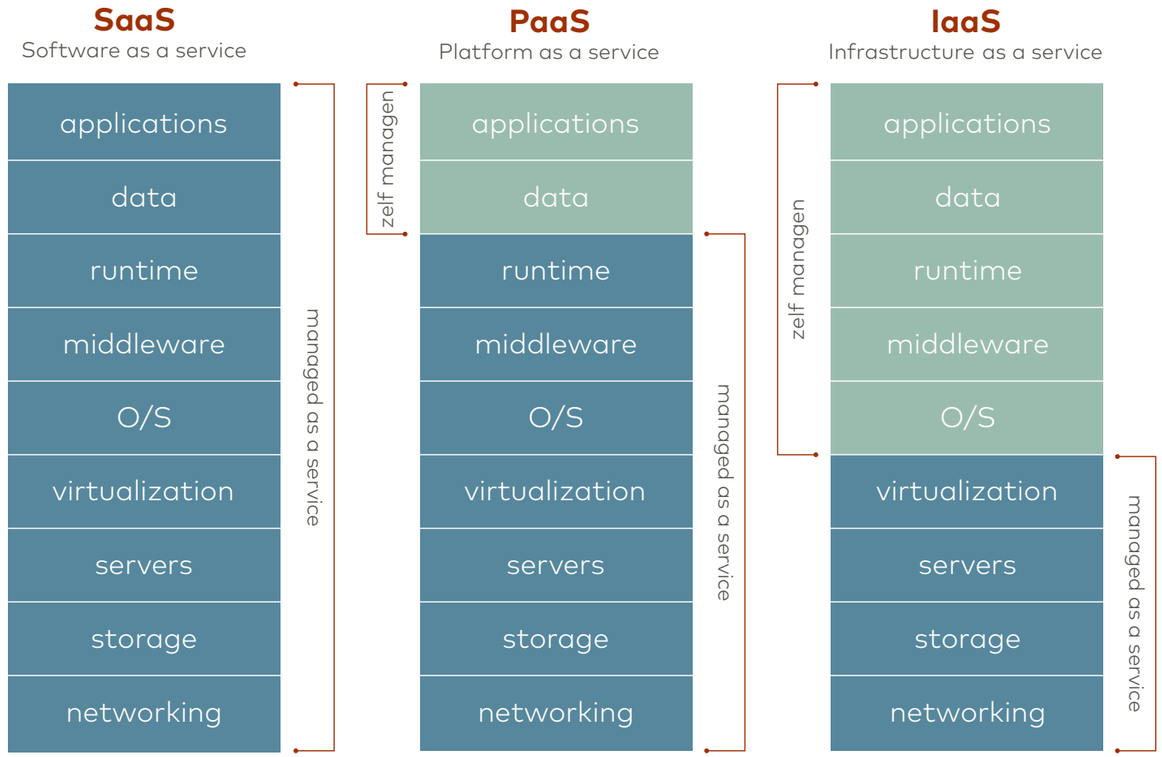
Flexibiliteit en schaalbaarheid

Flexibiliteit en schaalbaarheid zijn belangrijke voordelen, maar tegelijkertijd is het een kunst om als organisatie wel 'in control' te blijven. Als de situatie erom vraagt, wilt u in staat zijn uw workload snel te verplaatsen, zonder dat hier hoge kosten of risico's tegenover staan. Niet voor niets is de multicloud de afgelopen jaren steeds nadrukkelijker op de IT-agenda komen te staan.

Optimale flexibiliteit met de multicloud

Multicloud is de implementatie van een enkele afzonderlijke cloud-implementatie die meerdere cloud-serviceproviders combineert (niet te verwarren met een hybride cloud). Het kiezen voor een multicloudaanpak zorgt dat u niet afhankelijk bent van één enkele serviceprovider en dat u flexibeler bent (doordat u meer keuze heeft).

2.Welk servicemodel past bij uw organisatie?



Wanneer u heeft besloten welke vorm van de cloud het best past bij uw organisatie, maakt u ook de keuze in hoeverre u het beheer van de IT-omgeving uit handen geeft. Aan de basis van de cloud staat 'Everything as a Service', ook wel XaaS. Hieronder vallen een aantal servicemodellen:

Software as a Service SaaS

Misschien wel de meest bekende 'as a Service' variant is software (SaaS). In plaats van het eenmalig aankopen van software betaalt u de software naar gebruik. De meeste SaaS-oplossingen worden direct online gebruikt zonder dat er een download of installatie nodig is. Ook heeft SaaS als voordeel dat de leverancier het beheer en de opslag van de applicatie verzorgt en dat nieuwe functionaliteit centraal wordt ontwikkeld en voor alle gebruikers op hetzelfde moment beschikbaar komt.

Tegenwoordig is er een breed scala aan applicaties via het internet te gebruiken: van kantoorsoftware (Microsoft Office 365, Salesforce.com) tot boekhoudpakketten (AFAS Software, Exact), HRsoftware (WorkDay) en ERP applicaties (SAP, Oracle).

Platform as a Service PaaS

Wanneer organisaties een platform online afnemen waarop ze maatwerk applicaties kunnen ontwikkelen, dan spreken we van Platform as a Service (PaaS). Een PaaS-platform bestaat uit gedeelde hardware voor server en gegevensopslag inclusief de benodigde virtualisatie software en besturingssystemen.

Het onderhoud en beheer zijn voor rekening van de cloud provider. In tegenstelling tot SaaS dient u bij PaaS meer beheerderstaken zelf uit te voeren. Dit vergt meer kennis en ervaring. De meest bekende PaaS aanbieders zijn Amazon (EC2), Microsoft (Azure), Oracle en Google (App Engine).

Infrastructure as a Service IaaS

Een IaaS-oplossing biedt uw organisatie een virtuele hosting omgeving met controle over onder andere gegevensopslag, netwerkapparatuur en besturingssysteem. U betaalt alleen voor wat u daadwerkelijk gebruikt. Groot voordeel is dat de extra capaciteit vrijwel onmiddellijk beschikbaar is en u niet zelf hoeft te investeren in hardware en de locatie van een server. Publieke IaaS partijen zijn Amazon (AWS), Microsoft (Azure), Google Cloud Platform en Oracle (NetApp).

Als u de stap naar de cloud gaat maken of uw cloudomgeving gaat uitbreiden brengt dit een aantal uitdagingen met zich mee. Welke applicaties, data en platformen gaat u waar onderbrengen?

3. Aandachtspunten bij cloudmigratie

Nu u een beter beeld heeft van de cloud is het tijd om de eigen IT-omgeving goed te inventariseren. Migreren naar de cloud is een complex proces. U heeft immers te maken met verschillende applicaties en systemen die overgezet moeten worden.

"Betrek diverse zorgcollega's bij een inventarisatie"

Denk daarom van te voren goed na hoe u dit proces gaat inrichten. Welke applicaties gaan in de cloud? En gaat u meerdere clouds gebruiken? Dan krijgt u wellicht te maken met uiteenlopende leveranciers van SaaS, PaaS en IaaS. Gaat uw afdeling deze partijen vervolgens zelf aansturen of besteedt u dit liever uit?

Zorg voor een volledige inventarisatie

Bij de migratie naar de cloud start u met de inventarisatie van uw huidige IT-omgeving. Maar let op: een goede inventarisatie gaat verder dan een lijst maken van applicaties en systemen. Uw medewerkers en de verschillende afdelingen gebruiken meer IT-oplossingen dan de IT-afdeling vaak beseft. Denk bijvoorbeeld aan clouddiensten die ze privé al gebruiken, zoals Dropbox of Google Drive. Neem maatregelen om de wildgroei aan deze schaduw IT tegen te gaan. Dit doet u bijvoorbeeld door duidelijk te communiceren welke voorkeursleveranciers er zijn.

Betrek uw medewerkers en afdelingen ook bij de inventarisatie om inzicht te krijgen in de verschillende verwachtingen en belangen die meespelen. Zo komt u er achter waarom uw gebruikers geen gebruik maken van de door de organisatie aangeboden IT-oplossingen. Misschien is het zelfs tijd voor andere leveranciers?

Belangrijke vragen om binnen de organisatie te stellen

- Hoeveel vestigingen en werkplekken heeft u momenteel?
- Welke soft-en hardware gebruiken de medewerkers en afdelingen van uw organisatie?
- Is er overlap tussen verschillende applicaties en systemen?
- Kan de software ook vanuit de cloud worden afgenomen?
- Moet een aantal applicaties (maatwerksoftware of verouderde bedrijfskritische pakketten) toch op een eigen server blijven draaien?
- Of zijn er goede alternatieven in de cloud voorhanden?
- Wie verzorgt het beheer van uw IT-omgeving?
- Heeft uw IT-afdeling voldoende kennis om te migreren?
- Hoe wilt u de regie gaan voeren over de keten?
- Wat is uw beleid op het gebied van privacy & security?

Connectiviteit met de cloud

Als u een inventarisatie maakt, is het ook tijd om kritisch te kijken naar de huidige infrastructuur. Betrouwbare connectiviteit zijn een cruciaal onderdeel van de cloud. Neem daarom ook uw internet en netwerkdiensten onder de loep. Voldoen die straks in de praktijk als het gaat om bandbreedte, schaalbaarheid en beschikbaarheid?

Exit-strategie

Het laatste aandachtspunt is die van een succesvolle exitmogelijkheid. Wie van de ene naar de andere cloud provider over wil stappen, zal dat van tevoren goed moeten regelen. Bijvoorbeeld door in het contract met de cloud provider op te nemen dat de bedrijfsdata gemakkelijk en snel naar een nieuwe partij zijn over te hevelen, zónder dat daar extra kosten bij komen kijken.

Belangrijke vragen om tot een beslissing te komen

- Hoeveel aparte internet- en netwerkdiensten zijn er?
- Kunt u altijd bij uw gegevens?
- Is er rekening gehouden met redundantie?
- Geeft de netwerkleverancier ook de nodige garanties op de continuïteit van zijn dienstverlening?
- Is de netwerkleverancier in het bezit van certificeringen die de kwaliteit garanderen?
- Wat zijn de adviezen van de cloud providers op het gebied van verbindingen qua bandbreedte en kwaliteitseisen?
- Hoe gaat u de connectiviteit naar deze platformen of applicaties organiseren?
- Hoe belangrijk zijn deze voor de continuïteit van uw organisatie?
- Hoe waarborgt u de security van uw IT-omgeving?
- Hoe schaalbaar zijn uw connectiviteitsdiensten?

4. Veilige connectie

Een betrouwbare en veilige netwerkverbinding is van cruciaal belang voor toegang tot uw cloudomgeving. U kunt op twee manieren verbinding maken met de cloud: via het publieke internet of via een privé netwerk. In dit laatste geval maakt u gebruik van de diensten van een netwerkleverancier. In dit hoofdstuk lichten we de voor- en nadelen van deze diensten toe, zodat u een juiste keuze kunt maken.

"Kiest u in de zorg voor een publiek- of privé netwerk?"

Via het publieke netwerk

Het publieke internet lijkt de eenvoudigste manier voor organisaties om met de cloud te verbinden. Helaas kleven er behoorlijk wat nadelen aan deze oplossing:

- Er is geen controle over de verschillende 'tussenstations' waar de bedrijfsdata en -applicaties overheen gestuurd worden. Een echte Quality of Service (QoS) op de verbinding is bij het publieke internet niet af te geven.
- De schaalbaarheid is beperkt. Snel opschalen bij pieken in het gebruik van cloudapplicaties is er niet bij. U heeft dus een redelijke bandbreedte nodig om extra capaciteit op te kunnen vangen.
- De beveiliging is niet waterdicht. Als u een beveiligde cloudverbinding wilt realiseren zult u extra moeten investeren in een beter beveiligde verbinding.
- Aansluitend zult u het netwerk nog moeten verbinden met een cloud provider naar keuze.

Via een privé netwerk

Als u kiest voor een privé netwerk voor toegang tot de cloud, verloopt uw dataverkeer via een privé verbinding over een gesloten netwerk. De verbinding met de cloud wordt in feite onderdeel van uw bedrijfsnetwerk. Er zijn hierin twee mogelijke manieren van aanpak: U kunt een privé netwerk volledig zelf inrichten of gebruik maken van een netwerkleverancier.

In beide gevallen heeft u hoogwaardige connectiviteit nodig.

Wanneer u het zelf inregelt, is er uitgebreide expertise en specialistische kennis nodig. Er moeten verbindingen worden gerealiseerd en rackruimte gehuurd en ingericht worden in datacenters waar de verschillende cloudplatformen draaien.

Veiligheid voorop

Uiteraard mag innovatie nooit ten koste gaan van de veiligheid. Maar nu steeds meer bedrijven afhankelijk zijn van hun data en die steeds vaker via de Cloud en het internet transporteren is security een superbelangrijk issue geworden. Zeker als het om bedrijfskritische informatie en applicaties gaat.

Maar hoe veilig is dat datatransport eigenlijk? Wie zeker wil zijn dat zijn data 24/7 bereikbaar is en beveiligd is als Fort Knox, doet er goed aan om te kiezen voor een veilig en betrouwbaar glasvezelnetwerk. Dit kan bijvoorbeeld door een volledig geïsoleerd privé netwerk dat nergens het internet op gaat en dus onbereikbaar voor kwaadwillende actoren wordt. Of via een beveiligde en directe connectie met toonaangevende cloudserviceproviders.

Ook is er kennis nodig over de verschillende netwerklagen, BGP protocollen en IP routering om met de cloudplatformen te koppelen. Waarna u de cloudomgeving kunt gaan bouwen en inrichten.

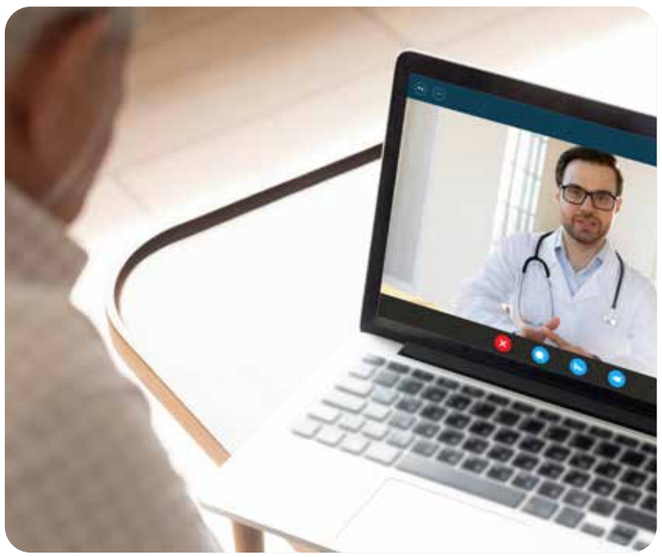
Het alternatief is dat u gebruik maakt van de diensten van een netwerkleverancier voor een IaaS connectiviteitsoplossing. Deze levert u privé verbindingen met de datacenters van de diverse cloud providers over hun vooraf ingerichte infrastructuur, dit biedt u een aantal voordelen:

- Goede toegangsbeveiliging tot uw applicaties en data in de cloud. Namelijk, het netwerk wordt opgezet op basis van private Ethernet of IP VPNverbindingen en is volledig gescheiden van het publieke internet. (lees meer over VPN in het kader op deze pagina)
- Een één op één relatie met de netwerk-leverancier, met een Service Level Agreement (SLA), specifiek voor de afgesloten dienstverlening.
- Sommige netwerkleveranciers bieden een end-to-end koppeling via hun netwerk met aangesloten cloud providers, geheel ingeregeld op een cloud exchange of directe koppelingen met de diverse cloud providers. Deze complete oplossing biedt daarbij redundantie naar de cloud, zeer hoge beschikbaarheid en niet onbelangrijk, een dienst tegen relatief lage kosten. Het enige waar u zorg voor moet dragen is de inrichting van uw cloudomgeving. Deze oplossingen passen volledig in het cloudmodel van ontzorgen, schaalbaar-heid en flexibiliteit. En u hoeft zelf niet de specialistische netwerkkennis in huis te hebben om direct met cloud providers te koppelen of een datacenter infrastructuur in te richten.

Wat is VPN?
VPN staat voor Virtual Private Network: een virtueel datanetwerk tussen locaties, dat gescheiden is van het publieke internet. Met VPN-verbindingen creëert u een gesloten organisatienetwerk tussen uw hoofdkantoor, vestigingen en datacenters. Het netwerk is eenvoudig uit te breiden en stimuleert efficiënt werken.

De voordelen van een VPN
- U kunt meerdere diensten over uw VPN-verbinding transporteren, zoals internet, telefonie en video. Door ook uw datacenters via het netwerk te ontsluiten, is het mogelijk om applicaties en platformen centraal aan te bieden.
- Voor uw organisatienetwerk kunt u per verbinding de behoefte aan bandbreedte bepalen. Zo bent u flexibel tijdens piekmomenten.
- U kunt uw hoofdkantoor, vestigingen en in- of externe datacenters via enkelvoudige of redundante verbinding-en aan elkaar koppelen. Het belang van de locatie bepaalt welk type connectivi-teit u nodig heeft.

"Toekomst-bestendige oplossingen"



5. Securitybeleid

De cloud en de verbindingen ernaartoe vragen om een modern en toekomstbestendig securitybeleid. Een beleid dat alle nieuwe verbindingen en opslagmogelijkheden zo goed mogelijk beschermt tegen cybercriminelen. De gevolgen van een cyberaanval kunnen een ramp zijn voor uw organisatie. Hoe zorgt u ervoor dat u uw organisatie zo veilig mogelijk inricht?

"Juist voor de zorg geldt: veiligheid voor alles"

De financiële gevolgen van een cyberaanval

Op het moment dat een cybercrimineel uw organisatie binnendringt, heeft dit grote gevolgen. Cybersecurityspecialist Kaspersky heeft onderzocht dat de kosten na een cyberaanval bij bedrijven uiteenlopen van 120.000 dollar tot wel 59 miljoen dollar*.

Een deel van die kosten zijn direct gerelateerd aan de naweeën van de cyberaanval, zoals het dichten van het lek en het inhuren van security-experts. De grootste kosten ontstaan echter door omzetverlies en reputatieschade. Uw organisatie wordt in een negatief daglicht gesteld.

En dat is nog niet alles. Mogelijk ontvangt u claims van derden. En daarnaast kunt u ook nog een flinke boete opgelegd krijgen door de overheid. In de Europese Unie verplicht de Algemene Verordening Gegevensbescherming een datalek binnen 72 uur te melden. Doet u dit niet, of doet u dit te laat, dan kan de boete oplopen tot 20 miljoen euro, dan wel 4 procent van de wereldwijde jaaromzet van de onderneming**.

Wat de kosten voor uw organisatie zullen zijn, is natuurlijk erg afhankelijk van het soort en de omvang van uw organisatie en ook de vorm van de cyberaanval. Wij adviseren u dan ook om u vooraf te laten adviseren door een securityspecialist.

Security in de cloud

Als u een clouddienst afneemt, liggen veel cybersecuritymaatregelen op het bord van de cloud provider. Zij nemen security zeer serieus en investeren er flink in. Die investeringen variëren van fysieke beveiliging, toegangscontrole, gegevens-opslag tot en met continue training van gespecialiseerd personeel.

Daarmee gaan veel cloud providers verder dan een organisatie zelf zou kunnen. Natuurlijk moet u zelf ook maatregelen nemen om de kans op een cyberaanval te verkleinen. Zoals het inrichten van een Cyber Threat Management platform of het afnemen van een Security Operations Service. Zorg ook voor een passend antivirussysteem op al uw apparaten en laat updates regelmatig uitvoeren. En, misschien wel het belangrijkst: zorg ervoor dat uw medewerkers weten hoe zij veilig werken.

Leer ze wat wel en niet mag als het gaat om de toegang tot applicaties en data en leer hen hoe ze sterke wachtwoorden instellen. Organiseer bijvoorbeeld met regelmaat awareness sessies waarin ze leren omgaan met de risico's van cybercriminaliteit.

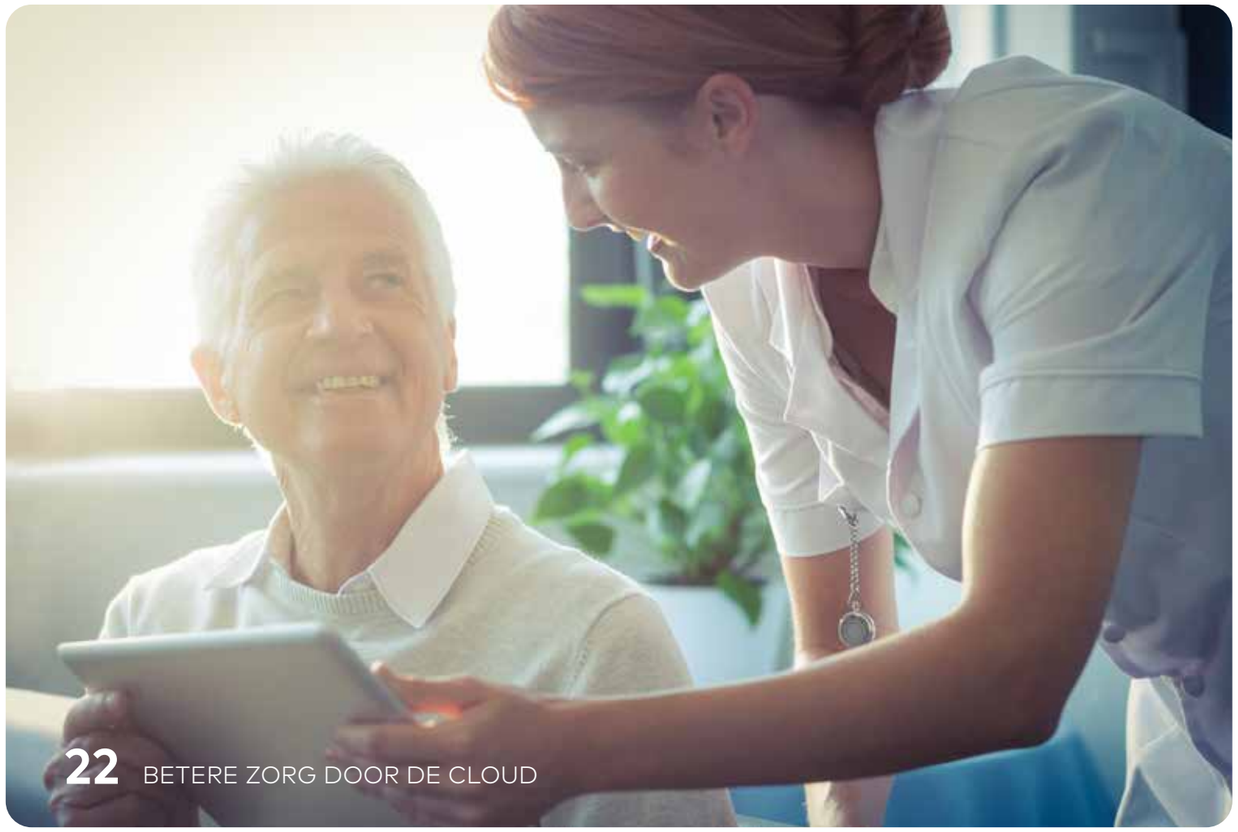
Verbindingen onderbelicht aspect van cybersecurity

De verbinding met de cloud is een onderbelicht element bij de beveiliging. Toch is het een essentiële schakel: alle applicaties en data lopen immers via de verbinding met de cloud provider. Dé ingang voor cybercriminelen om toe te slaan.

Houdt uw verbindingen daarom continu in de gaten door middel van monitoring. Zo kunt u verstoringen in het netwerk direct detecteren. Bij Ethernet en IP VPN- verbindingen is deze monitoring tweeledig: de leverancier heeft zicht op zijn eigen netwerk en u, als klant, heeft overzicht over het gehele stuk, inclusief uw eigen netwerk en de apparatuur die zich daarin bevindt. Als er storingen optreden, kan eenvoudig worden nagegaan of het een storing betreft naar aanleiding van (geplande) werkzaamheden of dat er iets anders aan de hand is. Bij alle netwerkapparatuur worden monitoringtools geleverd waarin onder meer latency, retransmissies en bit errors worden gemeten.

Beheer uw netwerkcomponenten en -poorten actief, zodat u bij latency veranderingen en onderbrekingen van het signaal direct alarmbellen ziet afgaan. Dit zijn indicaties dat er mogelijk ongewenste apparatuur in het netwerk is geplaatst. De grote aanbieders van de cloud hebben inmiddels oplossingen ontwikkeld voor directe en beveiligde toegang via een netwerkverbinding.

*Bron Kaspersky: https://usa.kaspersky.com
**Bron: https://autoriteitpersoonsgegevens.nl



"Cybersecurity in de zorg is vaak nog onderbelicht"

Encryptie is essentieel

Om te kunnen voldoen aan de AVG is encryptie onontbeerlijk. Encryptie versleutelt data, zodat, als het onverhoopt verloren of gestolen wordt, kwaadwillenden er niets aan hebben. Ze kunnen de data dan immers niet ontcijferen. Afhankelijk van de toepassing, kunt u op verschillende netwerklagen encryptie toepassen en dataverkeer versleutelen.

6. Secure Cloud Connect van Eurofiber

Om als organisatie wendbaar en flexibel te zijn, gaat u steeds meer vanuit de cloud werken. Met Secure Cloud Connect heeft u altijd veilig en direct toegang tot meerdere cloudplatformen. Met deze complete end-to-end oplossing krijgt u direct toegang tot de platformen van uw keuze via een veilig privé-netwerk.

Efficiënte totaaloplossing

We verbinden uw organisatie via een virtueel privénetwerk (VPN) met uw cloud providers, waarbij het netwerk volledig van het publieke internet is gescheiden.

Daarnaast krijgt u direct toegang tot het platform van uw keuze door middel van onze cloudkoppelingen. Eurofiber levert een end-to-end dienstverlening vanaf uw kantoorlocatie en/of datacenter locatie, naar publieke cloudservice providers zoals: Microsoft Azure, Microsoft Office 365, Amazon Web Services (AWS) en Google Cloud Platform. Andere cloudplatformen zijn beschikbaar op verzoek. Met Secure Cloud Connect beheert u alleen uw applicaties in de cloud, de rest regelen wij voor u.

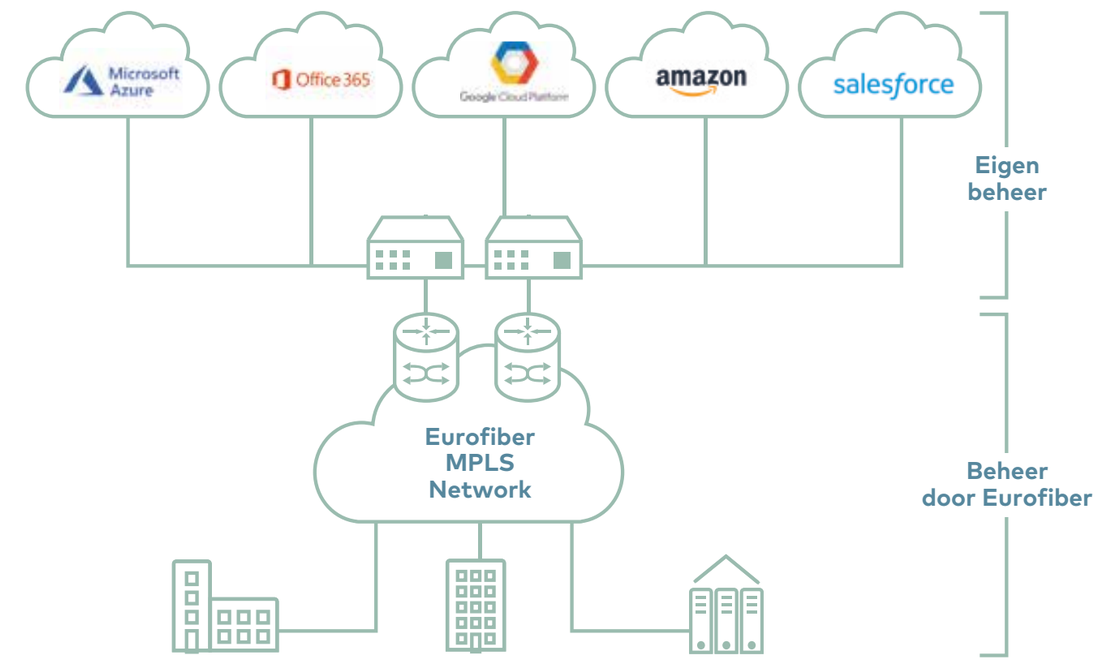
Op maat voor uw organisatie

We bieden u altijd een complete oplossing die optimaal aansluit op de situatie van uw organisatie. Wij adviseren u graag over het inrichten van uw netwerk: Internet, VPN-netwerk tussen uw hoofd- en nevenkantoren, datacenters en integratie van cloudservice providers.

U kunt uw netwerk flexibel inrichten per locatie naar bandbreedte, service level en enkele of redundante uitvoering. Secure Cloud Connect ondersteunt alle bandbreedtes van de diverse cloudservice providers van 50 Mb/s tot 10 Gb/s, zowel single als redundante aansluitingen.

Optimale beschikbaarheid en support

Om uw organisatie betrouwbaar toegang te bieden tot uw cloud providers, leveren we Secure Cloud Connect altijd over de glasvezel infrastructuur van Eurofiber en het Eurofiber private laag-2 netwerk. Daarnaast kunt u rekenen op 24 x 7 ondersteuning door ons Network Monitoring Center (NMC).



7. Het glasvezelnetwerk van Eurofiber

Eurofiber levert high-end connectiviteitsdiensten op basis van glasvezel voor de zakelijke markt. Eurofiber loopt voorop in het implementeren van nieuwe technologie en het continu verhogen van de kwaliteit van het glasvezel-netwerk.

Eurofiber Nederland

Eurofiber exploiteert sinds 2000 hoog-waardige digitale open infrastructuur. Met ons eigen glasvezelnetwerk en onze datacenters bieden we bedrijven, over-heden en non-profit organisaties een toekomstvaste, slimme en open infrastruc-tuur. Klanten hebben de vrijheid om zelf de diensten, toepassingen en aanbieders te kiezen die ze nodig hebben. Zo kunnen ze het innovatiepotentieel in de digitalisering ten volle benutten.

Naast het uitgebreide glasvezelnetwerk in Nederland en België en eigen datacenters in Nederland bieden we ook oplossingen voor interconnectiviteit tussen bijna alle hoogwaardige carrier neutrale datacenters in de Benelux. Eurofiber legt hiermee het fundament onder de digitale samenleving.

De Nederlandse overheid heeft Eurofiber dan ook de status toegekend van 'vitale infrastructuur'.

Flexibel en schaalbaar

Ons open netwerk geeft uw organisatie volledige vrijheid en flexibiliteit. U heeft de vrijheid om zelf de diensten, toepassingen en aanbieders te kiezen die u nodig heeft. Tevens biedt Eurofiber managed diensten op basis van het glasvezelnetwerk zoals WDM, Ethernet en Internet.

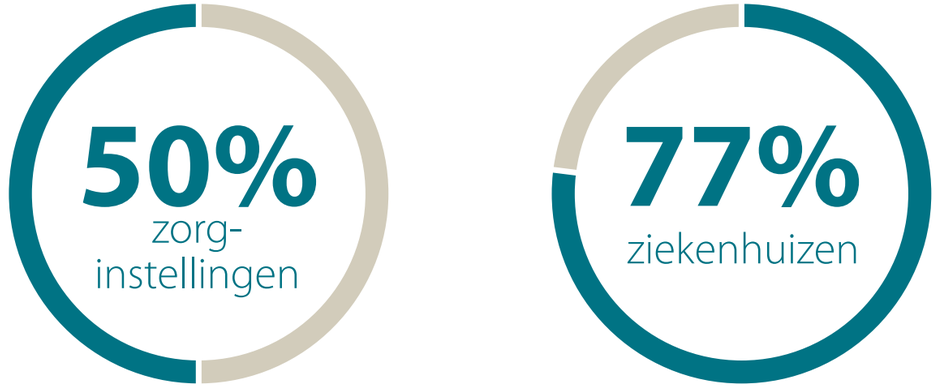
Veilig ondergronds netwerk

Het netwerk van Eurofiber ligt ondergronds op een diepte van 60 centimeter. Het werk aan ons netwerk gebeurt via gecertificeerde processen, die we continu controleren en jaarlijks toetsen.

We werken met gecertificeerde medewer-kers en aannemers. Op het netwerk is een Remote Fiber Test Systeem (RFTS) geïnstalleerd dat continu de beschikbaar-heid van de infrastructuur bewaakt. Bij een onverhoopte kabelschade door bijvoorbeeld graafwerkzaamheden kan het RFTS dan exact meten waar de breuk zich bevindt. Om verstoringen voor onze klanten te voorkomen, wordt regelmatig preventief onderhoud verricht om de netwerkkwaliteit te garanderen.

Hoge beschikbaarheid

De beschikbaarheid van het glasvezelnet-werk van Eurofiber is minimaal 99,9%. Als u kiest voor een volledig gescheiden tweede glasvezelroute (redundantie), bedraagt deze beschikbaarheid minimaal 99,99%. Als u twee gescheiden glasvezel-verbindingen heeft, garanderen wij dat wij nooit aan beide verbindingen tegelijkertijd werkzaamheden uitvoeren. Uiteraard informeren wij u, als klant, wanneer er werkzaamheden aan het netwerk zijn gepland.



Maakt gebruik van de redundante glasvezelverbindingen van Eurofiber

Innovatief in de zorg

De druk in de zorg was al hoog, maar door corona kwam er nog een flinke schep bovenop. Hoewel innovatieve ontwikkelingen als, domotica, hospital to the home, eHealth en patiëntportalen al volop in gebruik zijn, zorgde de pandemie ervoor dat de zorg op afstand versnelde, er meer virtuele zorg kwam en dat beeldconsults routine werden. Veel zorginstellingen kunnen innovatief zijn doordat zij eerder al flink hebben geïnvesteerd in een solide IT-netwerk. Al deze technieken vragen immers om extreem snelle en veilige verbindingen zonder vertraging. Slimme zorg die mogelijk is door een open glasvezelinfrastructuur.

LIFELINE

Netwerk Monitoring Center

U kunt rekenen op de 24/7 ondersteuning van de experts op het Eurofiber Network Monitoring Center. Het Netwerk Monitoring Center is gevestigd in Nederland en wordt bemand door Nederlands- en Engelssprekende experts.

Gegarandeerde reparatietijd

Het geografisch vastgelegde Eurofiber glasvezelnetwerk gecombineerd met de actieve bewaking van het Netwerk Monitoring Center zorgt ervoor dat de gegarandeerde reparatietijd op glasvezelverbindingen maximaal 8 uur is. Bij actieve diensten bedraagt deze maximaal 4 uur.

Beschikbaar in vrijwel elk datacenter van Nederland

Het Eurofiber glasvezelnetwerk is beschikbaar in een groot aantal datacenters in Nederland. Met de additionele Datacenter Services van ons zusterbedrijf Dataplace, met moderne Tier3-datacenters in de regio's Amsterdam, Rotterdam, Utrecht, Arnhem en Brabant, ondersteunen wij u met hoogwaardige colocatie oplossingen voor veilige huisvesting voor uw bedrijfskritische informatie en systemen.

Garanties

Eurofiber levert connectiviteit op basis van een Service Level Agreement. Hierin is exact vastgelegd welke prestaties, kwaliteitsniveau en garanties u van ons kunt verwachten. Duidelijke afspraken dus, zodat u altijd weet waar u aan toe bent.

Voor meer informatie kunt u contact met ons opnemen:
Safariweg 25-31, 3605 MA Maarssen
+31 (0)30 242 89 93, info@eurofiber.nl
www.eurofiber.nl

Eurofiber. Lifeline for the digital society

eurofiber