LIFELINE

The cloud as integrated part of your ICT infrastructure

Discover the possibilities for a safe
and direct access to the cloud

eurofiber

Foreword

The technology revolution we are currently experiencing is creating lightning-fast changes in market requirements. Your customers are forever making higher demands on you and they always expect you to use the very latest technological capabilities available. Those capabilities are also developing at bewildering speed: the new, versatile generations of businesses are constantly bringing new elements in their service concept to market. And it is vital for your organisation to respond quickly to all of these changes. But how do you do it? Just how do you give your organisation the flexibility and agility it needs?

The cloud makes it easier, cheaper and provides a lower entry level method for you to speed up the way you do business and to try out new things with your company. And because your time to market becomes shorter through the cloud, this also contributes to your competitive edge. In this e book we take you with us into this exciting new world. What exactly is the cloud? What are the benefits for your organisation? And why is security even more important with the cloud than it is in our traditional IT landscape? Discover the possibilities of cloud computing and find out how you can access multiple cloud platforms directly and securely.

Contents

The rise of cloud computing

Most organisations in Belgium use cloud computing to a greater or lesser extent. 91% of all ICT managers worldwide expect to implement cloud applications within the next 12 months. Yet there are many different types of cloud applications. So, what exactly do we understand by "the cloud"?

What is cloud computing actually?

The "cloud" is an off-site network to which many computers are connected... somewhere: "in the cloud", for want of a better term. And in the cloud is where all sorts of applications run. Which means that users no longer actually own the hardware and software they use, but then nor do they have to worry about maintenance any longer. What users have is their 'own' virtual infrastructure that is scalable in size and capabilities, somewhere they can go online to use the applications, software and data provided by data centers.

The benefits for your organisation

As a result, organisations and ICT managers in Belgium expect a great deal from the cloud. Are those expectations truly justified? You bet they are!

More flexible and agile

The cloud offers you an amazingly high level of flexibility and scalability. For example, upscaling and downscaling the users of an application often literally takes just a few clicks of the mouse. This makes your IT a versatile tool during peaks and troughs in your demand – instead of a financial and operational burden. The same applies for adopting new applications or services, as these are available on demand. The cloud also benefits the speed and agility of your organisation, for example when developing a new product or service.

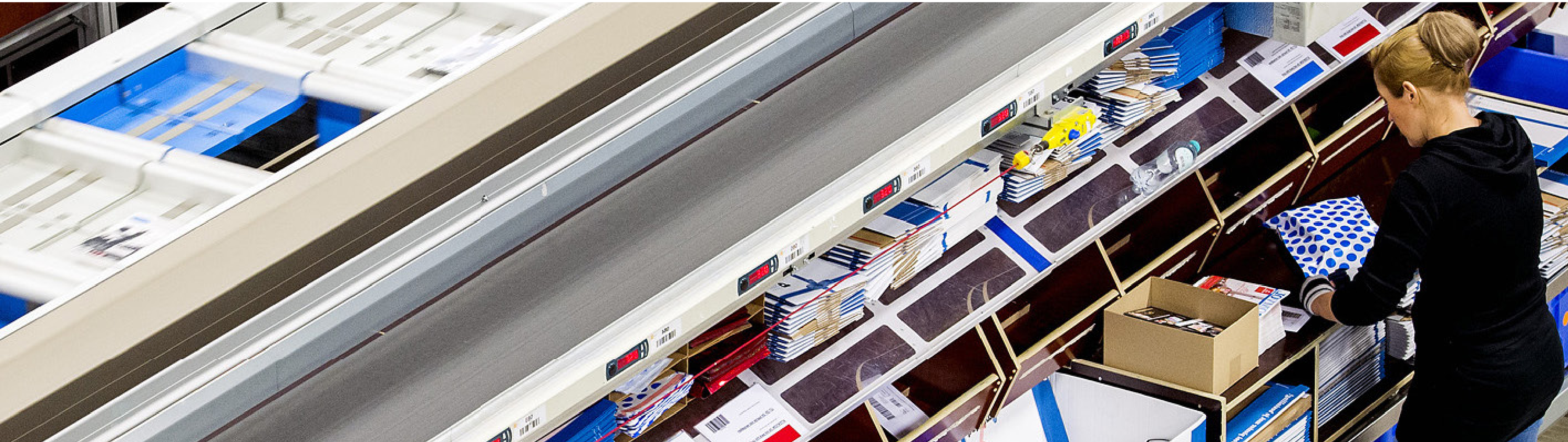
And, finally, cloud computing enables organisations to grow quickly: the extra IT capacity is available immediately when needed. Plus no investments are required to bring in extra servers and there are no problems with lengthy turnaround times.

Savings on IT costs

You may not always have noticed it, but sometimes large amounts of time and money are spent just managing and maintaining your own IT environment. With cloud computing, it's the cloud provider that makes the capital and labour-intensive investments: from purchasing network servers and applications, to taking security measures. And things such as maintaining a team of highly qualified IT specialists are all the responsibility of the cloud provider.

If you decide to cancel a particular cloud service, you only pay for what your organisation and staff actually use. There are various charging options, too: per month, per user or per resource consumed. This system means you make savings on your IT costs. To put it in financial terms: CAPEX (Capital Expenditure, investments) becomes OPEX (Operational Expenditure, current expenditure).

Of course, when you use cloud computing, you also need to keep a sharp eye on your spending. Be sure to conduct regular checks into which cloud services your user groups are consuming and make on demand adjustments to the services you use.



Switching to the cloud

Being able to respond quickly to changes and to cut back on costs is an important argument for making the move to the cloud. In fact, you will have a number of choices to make so that you can create the cloud environment that's best for you. The most important choice is whether to use the public, private or hybrid cloud.

3 user models: public, private

and hybrid cloud To cater for the differing requirements of organisations, there are three user models for the cloud: public, private and hybrid. Choose the model that best suits your requirements.

Public cloud

The name says it all: the public cloud can be accessed by anyone. The public cloud consists of a virtualised IT environment that enables different types of organisations to use their own individual IT environment, including the operating system. The cloud provider works with a number of standard configurations for network servers, cybersecurity, applications and data storage. The cost of managing and maintaining the IT is paid for by the cloud provider.

Advantages

- **Relatively low investment**
  Because it has standard configurations, the cloud provider is able to service a significant number of customers. Which means that the pricing is relatively low.
- **Rapid rollout of new developments**
  Public cloud platforms have the ability to implement new developments quickly. That way, you benefit from any new capabilities sooner
- **Scalability**
  For short-term projects you can bring in extra storage space or boost your number- crunching abilities quickly.
- **A wealth of expertise about keeping information secure**
  Cloud providers usually have a high level of maturity when it comes to protecting data. This includes measures for physical security, access control, data storage and the on going training of specialist staff.

Disadvantages

- **Limited scope for customisation**
  Cloud computing means there is a wide range of applications and services available. These need to be tailored to the specific IT needs of your organisation.
- **Privacy considerations**
  With the public cloud, it is not always clear on what systems and in which countries your data is located. Sometimes the government requires organisations to retain certain items of data under their own management control at all times.

Private cloud

When the virtualised IT environment is used exclusively for one specific company, this is called a private cloud. With the private cloud, the cloud provider's applications and services are kept in a managed data center or at the provider's own data center. Just like with the public cloud. However, a private cloud is a totally fenced-off IT environment, with its own servers for applications and data storage. Your own IT department will usually handle the management and maintenance (if you require, this can be done by a special team provided by the cloud provider).

Advantages

- **Customised**
  The applications and services are geared to the needs of your organisation.
- **Privacy considerations**
  You always know exactly where your data is stored. This is crucially important for financial institutions, for example: legislation and the regulators require that they know exactly where the (client) data is located and how security is handled.

Disadvantage

- **Higher investment**
  The customisation required for a private cloud means that this solution may be more expensive than the public cloud. This is because of the extra investments required for hardware, physical protection and continuity. Another consideration are the higher costs for upscaling additional capacity.

Hybid cloud

The hybrid cloud is a combination of the public and private cloud, with the hybrid cloud offering you the best of both worlds. For instance, with the hybrid cloud you will use the standard offering of the public cloud, such as Microsoft Office 365. But in addition you will also use customisation solutions for complying with the privacy laws, or to enable you to continue using your own sector or company-specific software. This handy combination means that the hybrid cloud is becoming increasingly popular.

Advantages

- **Financially attractive standard configurations** with the speed and flexibility of the public cloud.
- **Customised solutions** for specific applications and systems, as in the private cloud.

Disadvantages

- **Higher level of investment** than with the public cloud.
- **Complexity of combining** the public and private cloud.

The service models of cloud computing

When you have decided which form of cloud computing best suits your organisation, you then need to decide the extent to which you outsource management of the IT environment. Based on cloud computing there is 'Everything as a Service', also known as XaaS, under which are a number of service models.

Software as a Service (SaaS)

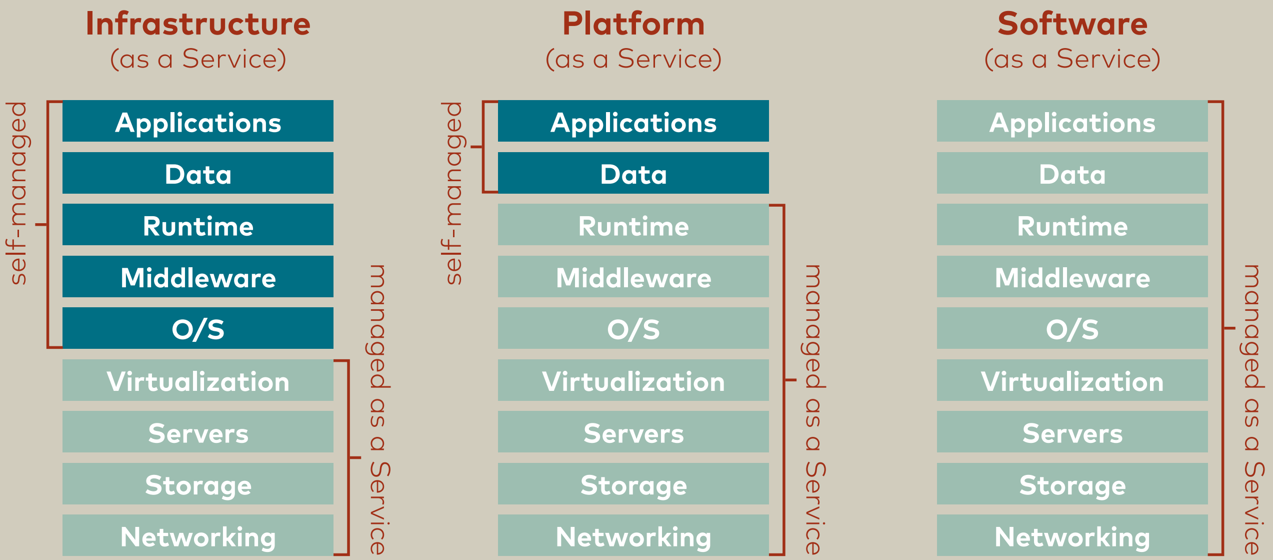
Probably the best-known 'as a Service' variant is Software as a Service (SaaS). Instead of paying the one-off cost of buying software, you simply pay for using the software. Most SaaS solutions are used directly online without the need for a download or installation. Another advantage of SaaS is that the provider also handles the management and storage of the application.

Currently there is a wide range of applications that can be used via the Internet:from office software (Microsoft Office 365, Salesforce. com) to accounting packages (AFAS Software, Exact), HR software and ERP applications (SAP, Oracle).

Platform as a Service (PaaS)

When organisations occupy a platform online where they can develop customised applications, this is called Platform as a Service (PaaS). A PaaS platform consists of shared hardware for server and data storage, including the necessary virtualisation software and operating systems. The maintenance and management are handled by the cloud provider. In contrast to SaaS, with PaaS you have to carry out more of the manager tasks yourself. This offers you flexibility, but requires more knowledge and experience.

The best-known PaaS providers are Amazon (EC2), Microsoft (Azure), Oracle and Google (App Engine).



Infrastructure (as a Service)

self-managed: Applications, Data, Runtime, Middleware, O/S

managed as a Service: Virtualization, Servers, Storage, Networking

Platform (as a Service)

self-managed: Applications, Data

managed as a Service: Runtime, Middleware, O/S, Virtualization, Servers, Storage, Networking

Software (as a Service)

managed as a Service: Applications, Data, Runtime, Middleware, O/S, Virtualization, Servers, Storage, Networking

Infrastructure as a Service (IaaS)

An IaaS solution offers your organisation a virtual hosting environment with control over areas such as data storage, network equipment and operating system. You only pay for what you actually use. One major advantage is that the additional capacity is available virtually immediately and there is no need for you to invest in hardware or leasing a server.

Known IaaS providers are Amazon (AWS), Microsoft (Azure), Google Cloud Platform, IBM SoftLayer and Oracle (NetApp).

There are a number of challenges to consider when you make the move to the cloud or expand your cloud environment, such as what applications, data and platforms are you going to accommodate, and where?

Key issues when migrating to the cloud

Now that you have a better idea of what cloud computing is all about, it's time to take a close look at your own IT environment. Migrating to the cloud is a complex process, because various applications and systems have to be moved. So think carefully about how you intend to tackle this process. What applications will be going to the cloud? And will you be using more than one cloud? Then you will have to deal with the various providers of SaaS, PaaS and IaaS. Will you want to deal with these providers yourself, or would you prefer to outsource the whole thing?

Carry out a full inventory

When migrating to the cloud you need to start by carrying out an inventory of your current IT environment. But beware: a proper inventory goes well beyond just making a list of your applications and systems. Your employees and the various departments often tend to use more IT solutions than the IT department realises. For instance, there are the cloud services that they may already be using privately, such as Dropbox or Google Drive.

So take measures to prevent the uncontrolled growth of this shadow IT. You can do this by making it clear which your preferred providers are. When drawing up your inventory, also involve your staff and departments so that you can discover what their differing expectations are and the various interests at play. This also enables you to find out why your people are not using the IT solutions provided by the organisation. Who knows, it may even be time for you to bring in other providers?

Sample questions that you need to be asking yourself when making an inventory

- How many locations and workstations do you currently have?
- What software and hardware are used by your organisation's staff and departments?
- Is there any overlap between the various applications and systems?
- Can the software also be taken from the cloud?
- Are there any applications (customised software or out-of-date business-critical packages) that need to be kept running on your own server? Or are there good alternatives available in the cloud?
- Who handles the management of your IT environment?
- What knowledge does your IT department have and is it sufficient if you intend to migrate?
- How do you want to handle control over the chain?
- What is your policy on privacy & security?

Connections to the cloud

When you are making an inventory, it is also a good time to take a critical look at your current infrastructure. Reliable connections are a crucial part of cloud computing. So take a close look at your Internet and network connections. For instance, are they sufficient when it comes to bandwidth?

Think about

- How many separate Internet and network connections are there?
- Can you always access your data?
- Is redundancy taken into account?
- Does your network provider also offer the guarantees you need regarding the continuity of the service it provides?
- Does the network provider have the relevant certification to guarantee quality?
- What are the recommendations of the cloud providers in the area of connections in terms of bandwidth and quality requirements?
- How do you intend to organise connectivity to these platform or applications?
- How important are they for the continuity of your organisation?
- How do you ensure the security of your IT environment?

Exit strategy

The final key issue is to make sure you have a successful exit option in place. If you want to move from one cloud provider to another, things need to be arranged properly in advance. For example by including in the contract with your cloud provider that your business data must be transferred quickly and easily to a new party. Without extra costs.

Connecting securely

A reliable, secure network connection is absolutely vital for accessing your cloud environment. There are two ways of connecting with the cloud: via the public Internet or via a private network. In this latter case, you will use the services of a network provider. In this section we explain all about the pros and cons of these connections so that you can make the right choice of what you want.

Via the public network

The public Internet would seem to be the simplest way for organisations to connect with the cloud. Unfortunately, this solution involves all sorts of disadvantages.

- You have no control over the various 'intermediate stations' through which your business data and applications will be sent. No genuine Quality of Service (QoS) can be given on the connection via the public Internet.
- Scalability is limited. You can't upscale quickly when there are spikes in your use of cloud applications. This means you will require reasonable bandwidth in order to accommodate any additional capacity required.
- Security is not watertight. If you want to make a secure cloud connection, you will have to invest more for a connection that has better security.
- You will also need to connect the network with a cloud provider of your choice.

Via a private network

If you opt for a private network to access the cloud, your data traffic will run via a private connection over a closed network. Your connection with the cloud will in fact become part of your business network. There are two possible ways of tackling this. You can set up your own private network yourself, or you can use a network provider. In both cases, you will need high-quality broadband connections.

If you organise access yourself, you will need a great deal of expertise and specialised knowledge. You need to arrange connections, lease rack space and organise data center where the various cloud platforms can run. You'll also need knowledge about the various network layers, BGP protocols and IP routing to connect with the cloud platforms. Once you have done all that, you will be able to start building and designing your cloud environment.

As an alternative, you can use the services of a network provider to create an IaaS connectivity solution. This provider will supply you with private connections with the data center of the various cloud providers over their established infrastructure. This in turn offers you a number of benefits.

- Good security for accessing your applications and data in the cloud. Specifically, the network is based on private Ethernet or IP VPN connections and is totally separate from the public Internet.
- A one-on-one relationship with the network provider, with a Service Level Agreement (SLA) specifically for the services provided.
- Some network providers offer a direct connection via their network to connected cloud providers, fully connected to a cloud exchange or direct links with the various cloud providers. This total solution also offers redundancy to the cloud and very high availability, as well as service at relatively low cost, which in itself is important. The only thing you have to worry about is the design of your cloud environment. These solutions fit closely into the cloud model, which is designed to relieve you of your concerns while offering scalability and flexibility. And better still, you don't need specialist network knowledge in-house to be able to connect directly with cloud providers or to set up a data center infrastructure.

What is VPN?

VPN stands for Virtual Private Network: this is a virtual data network between locations that is separate from the public Internet. With VPN connections you create a closed organisation network between your head office, other branches and data centers. The network is easy to expand and helps encourage efficient working.

The advantages of a VPN connection:

- You can carry various services over your VPN connection, such as Internet, telephone and video. By opening your data centers via the network it is also possible to offer applications and platforms centrally.
- For your organisation network you can set the bandwidth requirement for each connection. That means you can be flexible during peak times.
- You can also link your head office, other branches and internal or external data centers to each other via single or redundant connections. You define the importance of the location for the connection you need.

Checklist for direct cloud connections

A direct cloud connection means that you don't have to check the availability and security of the connection to the cloud. This choice is easy to make. But now how do you know which network provider to choose?

Essential questions when opting for a direct connection with the cloud

- □ Is there really a direct connection between your organisation and the cloud provider? Or are there any 'intermediate stations'? ______
- □ Does the direct connection with the cloud provider go via the provider's own network? ______
- □ Is the provider's network infrastructure redundant? ______
- □ What guarantee can the provider give regarding the availability of the connection? ______
- □ Does the provider assist you in choosing the optimum bandwidth? ______
- □ Is the provider able to implement the direct connections(s) on-site? ______
- □ How large is your current data volume and what will the expected data traffic be in the (near) future? ______
- □ How quickly can the bandwidth of the direct connection be upscaled? ______
- □ What service levels does the provider guarantee in the event of disasters or service disruptions? ______
- □ What does the escalation procedure look like in the event of disasters or service disruptions? ______
- □ Does the provider hold vital certification in cybersecurity (such as ISO 27001)? ______

Security policy

The cloud and the connections to it require a modern, future-proof security policy. A policy that protects all new connections and storage capabilities, as well as possible against cybercriminals. The effects of a cyber-attack can be a disaster for your organisation. How can you ensure that your organisation is set up as securely as possible?

The financial consequences of a cyber-attack

If a cybercriminal manages to penetrate your organisation, this will have major consequences on your business. Cybersecurity specialist Kaspersky Labs states that the costs after a cyber-attack can average anything between €45,000 and €580,000.

Part of these costs are directly related to the repercussions of the cyber-attack, such as plugging leaks and calling in security experts. However, the greatest costs are caused by loss of sales and damage to your reputation. Your organisation will be seen in a negative light, which means that your customers' trust will be adversely affected.

Security in the cloud

If you purchase a cloud service, many of the cybersecurity measures are the responsibility of the cloud provider. They take security very seriously and make investments to match. These investments vary from physical security, access control and data storage through to the ongoing training of specialised staff. As a result, many cloud providers go a great deal further than you would be able to as an organisation.

Of course you will have to take measures yourself to reduce the likelihood of a cyberattack. This will include setting up a Cyber Threat Management platform or purchasing a Security Operations Service. You will also need to install an appropriate antivirus system on all your equipment and implement regular updates. But perhaps the most important thing of all is to ensure that your staff know how to work securely. Show them what they must and mustn't do when it comes to accessing applications and data and teach them how to set up strong passwords. You could perhaps also organise regular awareness sessions at which they can find out more about dealing with the risks of cybercrime.

Connections: the often-ignored aspect of cybersecurity

Your connection with the cloud is a security element that is often ignored. Yet it is a vital link: all of your applications and data have to transit via your connection with the cloud provider. Which makes it the best point of entry for cybercriminals to get to work.

Network monitoring

For this reason, monitor your connections closely at all times. That way, you can detect disruptions in the network without delay. With Ethernet and IP VPN connections this monitoring is a two-way street: the provider will monitor its own network, while you as the customer have oversight of the whole system, including your own network and the equipment in it. If a problem occurs, you can easily check to see whether the disruption is the result of (planned) works or if something else is happening. Monitoring tools are provided with all network equipment to measure issues such as latency, retransmissions and bit errors. Be sure to manage your network components and ports actively, so that if there are any changes in latency or disruptions to the signal alarm bells will start ringing immediately. These are all indications that some undesirable devices may have been installed in the network.

The major providers of cloud computing have developed solutions for direct and secure access via a network connection.

To be able to comply with the provisions of the amended **Data Protection Act**, encryption is essential. Encryption scrambles data so that if it is inadvertently lost or stolen, cybercriminals can't do anything with it, because they are unable to decipher it. Depending on the application, you can apply various layers of network encryption and so lock away your data traffic from prying eyes.

Secure Cloud Connect from Eurofiber

To be increasingly agile and flexible, you will find yourself working more and more from the cloud. Secure Cloud Connect gives you secure and direct access to multiple cloud platforms at all times. This comprehensive solution gives you direct access to the platforms of your choice via a private network.

Efficient total solution

We connect your organisation via a virtual private network (VPN) with your cloud providers. This means your network is kept totally separate from the public Internet. You also get direct access to the platform of your choice via our cloud connections. We currently offer direct connections with leading cloud platforms such as Microsoft Azure and Microsoft Office 365. This will shortly be expanded to include other cloud providers, such as IBM SoftLayer, Google Cloud Platform, Amazon Webservices and well-known ERP and CRM providers, such as Salesforce, Oracle and SAP. With Secure Cloud Connect, all you have to do is purchase the cloud services you want from your provider. We'll do the rest for you.

Accessible platforms

• Microsoft Azure

Microsoft offers the Microsoft Azure cloud platform. Azure provides a comprehensive package of cloud computing services, from Infrastructure as a Service (IaaS) to fully managed Platform as a Service (PaaS). For example, it is possible to implement and scale the latest websites and web applications, manage SQL Database as a-Service or apply machine learning.

• Microsoft Office 365

Office 365 falls into the category of SaaS and is a typical example of cloud computing. Office 365 runs as an online service on any platform that supports the Internet.

• Amazon Web Services

Offering compute power, database storage, content delivery and other functionalities. AWS has the services to help build sophisticated applications with increased flexibility, scalability and reliability.

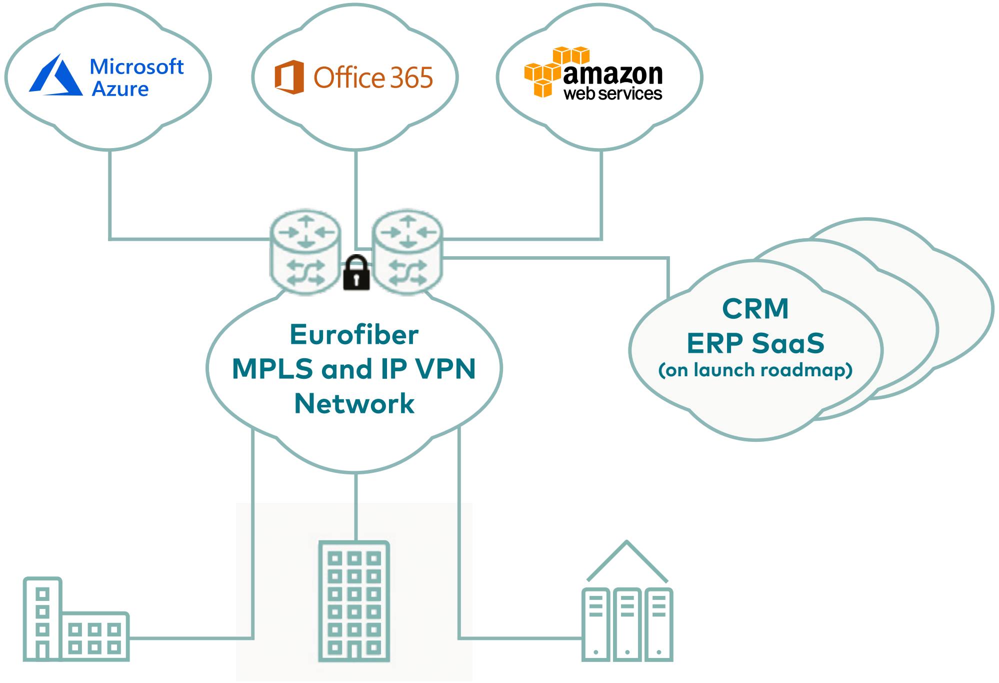
Tailored for your organisation

We always offer you a complete solution that fits exactly with your organisation. We are happy to advise you about setting up a VPN network between your head office and branches, data centers and cloud providers. You can set up this network flexibly by location, according to bandwidth, service level and as single or redundant system. You can also set up Cloud Connect to suit your needs.
The Secure Cloud Connect service is available in the following bandwidths.

50 Mb/s	100 Mb/s	200 Mb/s	500 Mb/s
1 Gb/s	2 Gb/s	5 Gb/s	10 Gb/s

Secure Cloud Connect and our fiber optic connections

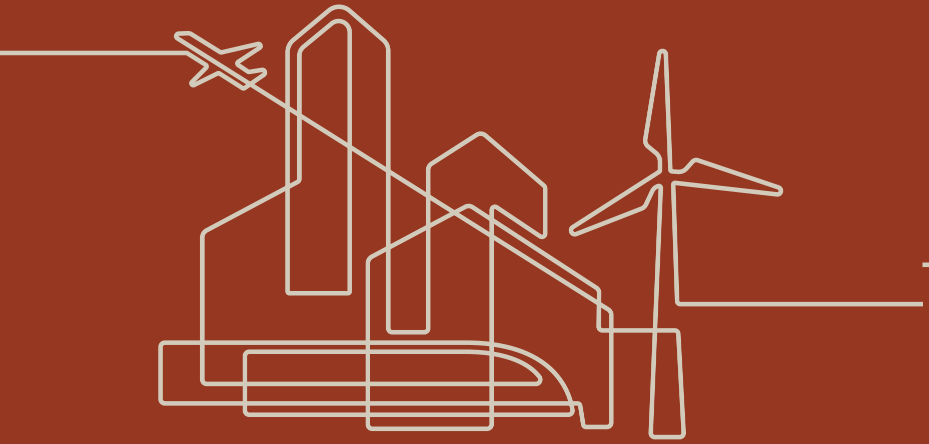
To provide your organisation with reliable access to your cloud providers, we always supply Secure Cloud Connect combined with our VPN services. And, of course we depend on the high-quality fiber option network of Eurofiber for all these services.



Curious to hear more about what we could achieve for your organization?

Eurofiber has been a fast-growing international provider of industry-leading digital infrastructure since 2000. Relying on our own fiber optic network and data centers, we provide smart, open, future-proof infrastructure to companies, government bodies and non-profit organizations. Customers have complete freedom to choose the services, applications and providers they need, allowing them to tap into the full potential of digital innovation. Eurofiber has an extensive fiber optic network in the Netherlands and Belgium, it unlocks its four data centers of its own and almost all public data centers in the Benelux.

This is a Lifeline eBook brought to you by Eurofiber. The Lifeline platform offers information and inspiration in the field of digital connectivity. Eurofiber.be/lifeline.



Eurofiber. Lifeline for the digital society

Fountain Plaza 504, Belgicastraat 5 bus 7,
1930 Zaventem, t +32 (0)2 307 12 00
info@eurofiber.be, www.eurofiber.be

eurofiber