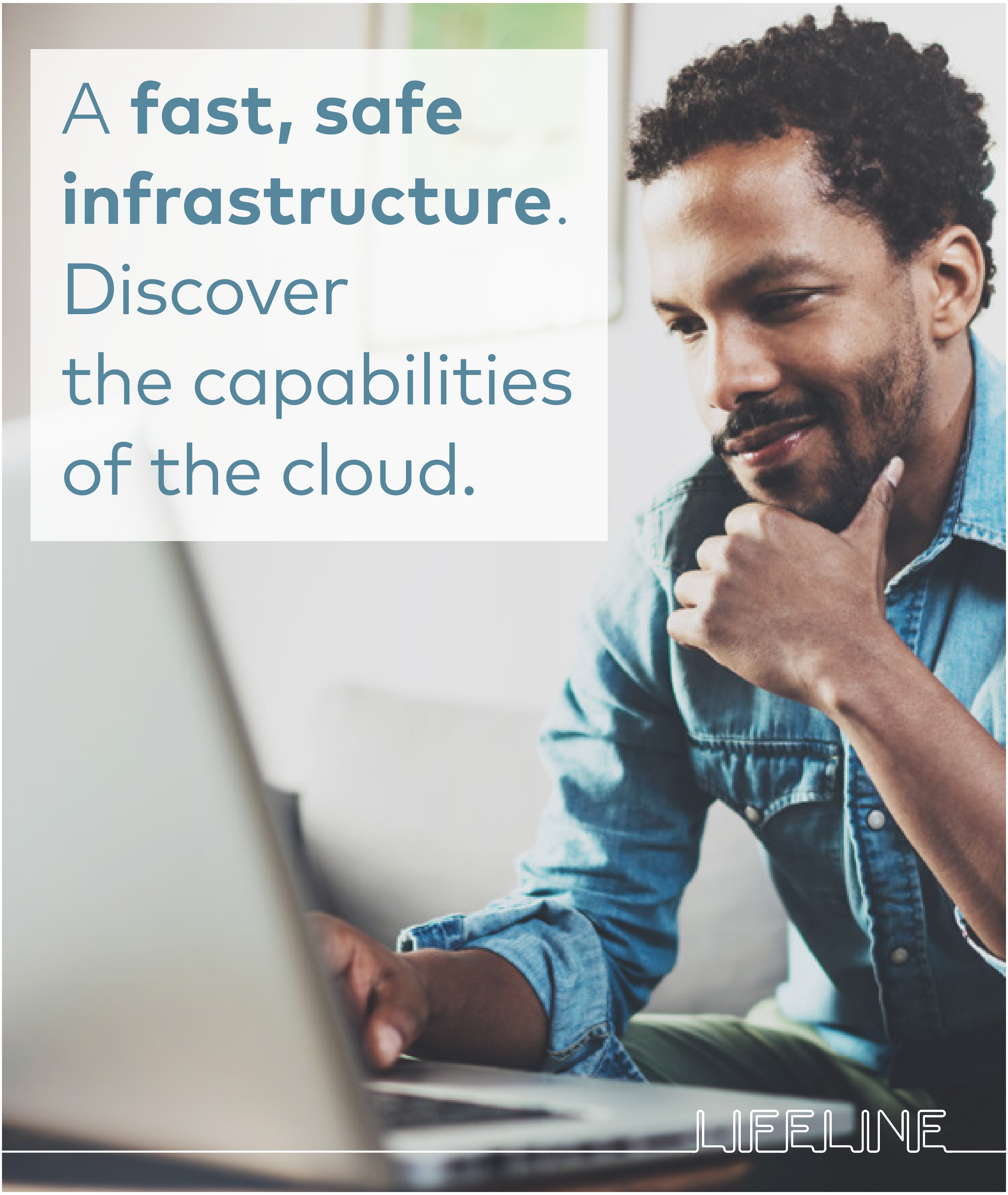
eurofiber

A **fast, safe infrastructure**. Discover the capabilities of the cloud.



How do you respond to rapidly changing societal demands?

Companies and organizations have a growing need for connectivity for all kinds of new applications. Just think of IOT, smart society, remotely controlled processes or robotics, simultaneously processing data from different locations, etc. Reliable connectivity is crucial.

The technological revolution we are currently experiencing creates rapidly changing demands in society. Those demands are constantly being increased and you are expected to use the latest technological capabilities.

Keeping up with all these developments requires an open infrastructure that serves as a foundation for today and tomorrow. But how do you do this? What do you need to look out for? How do you make your organization flexible and versatile?

The cloud makes it easier, more accessible and cheaper to speed up your organization. And due to the short time-to-market, the cloud contributes to your ability to adapt. In this e-book, we introduce you to this new virtual world. What is the cloud precisely? What are the benefits for your organization? And why is security even more important than in the traditional IT landscape? Discover the capabilities of the cloud and how to gain safe and direct access to multiple cloud platforms.

1

The growth of cloud computing

- What exactly is the cloud?
- The advantages for your organization
- Savings on IT costs

2

Switching to the cloud

- The three user models: public, private and hybrid cloud
- The service models of the cloud
  Software as a Service SaaS
  Platform as a Service PaaS
  Infrastructure as a Service IaaS

3

Points to consider when migrating to the cloud

- Make a complete inventory
- Connections with the cloud
- Exit strategy

4

Secure connection

- Via the public network
- Via a private network
- What is Ethernet VPN?

5

Security policy

- The financial consequences of a cyberattack
- Security in the cloud
- Connections neglected aspect of cybersecurity
- Network monitoring

6

Eurofiber's Secure Cloud Connect

- Efficient total solution
- Customized for your organization
- Optimal availability and support

1. The growth of cloud computing

Most organizations use the cloud to a greater or lesser degree. Recent research indicates that 94% of organizations have experience with the cloud. Of those organizations, 69% use the hybrid cloud, 22% the public cloud and 3% the private cloud. There are many types of cloud applications.

The cloud is a network of connected computers that form a "cloud of computers." An abundance of applications run on this network. Users are no longer owners of the software and don't have to worry about maintenance. Users have their 'own' virtual infrastructure, scalable in size and capabilities, with which they can make online use of applications, software and data that is offered from data centers.

The advantages for your organization

Organizations and IT managers expect a lot from the cloud. Is this justified? Definitely! The cloud offers lots of flexibility and scalability. For example, the open downscaling of users of an application is often a question of a few mouse clicks. As a result, when peak moments decline, your IT becomes a pleasant tool instead of a financial and operational obstacle. The same is true of using new applications or services; they are available on-demand. This is good for the speed and versatility of your organization when developing a new product or service for example. And working in the cloud enables an organization to grow in step with the desires of the general public. Extra IT capacity is available immediately, if required. Organizations don't have to invest in extra servers, for example, or cope with long lead times.

Savings on IT costs

A lot of time and money is spent on the management and maintenance of one's own IT environment without this being noticed. When working in the cloud, the cloud provider makes the capital-intensive and labor-intensive investments: from purchasing network servers and applications to taking security measures. Additional things like maintaining a team of highly-qualified IT professional are also the cloud provider's responsibility.

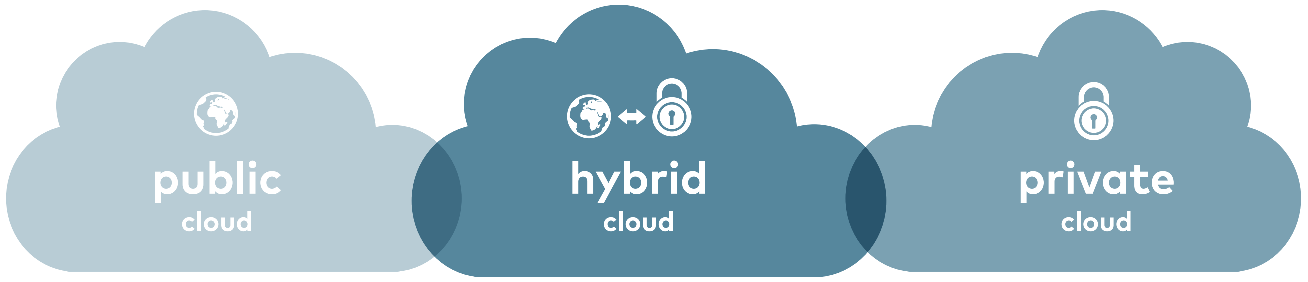
If you purchase a cloud service, then you only pay for what your organization and your employees use. There are different types of billing models: per month, per user or per purchased resource. This results in savings on your IT costs. To express it in financial terms: CAPEX (Capital Expenditure, investments) become OPEX (Operational Expenditure, ongoing expenses).

Of course, you still have to keep a close eye on your expenses with the cloud. You should periodically check which cloud services your user groups purchase and make on-demand adjustments in the purchased services.

2. Switching to the cloud

The need to respond quickly to changes and reduce costs are important arguments for switching to the cloud. You must make a number of choices in order to achieve an optimal cloud environment. Should you use a public, private or hybrid cloud?

The 3 user models:
Public, private and hybrid cloud. Because organizations have different requirements, providers offer different user models: public, private and hybrid cloud. Choose the cloud that is most suited to your requirements.



Public cloud

The name gives it away: the public cloud is accessible to everyone. This cloud consists of a virtualized IT environment in which different organizations each use their own IT environment, including operating system. The cloud provider works with a number of standard configurations for network servers, cybersecurity, applications and data storage. Management and maintenance of the IT environment are the responsibility of the cloud provider.

Advantages

- Relatively low investment
  Because they use standard configurations, cloud providers can serve a fair number of customers. This ensures relatively low pricing.
- Swift implementation of new developments
  Public platforms have the capacity to implement new developments quickly so you will immediately benefit from new opportunities.
- Scalability
  For temporary projects you can quickly deploy extra storage space or computing power.
- Lost of expertise on information security
  Cloud providers often have a high degree of maturity in terms of information security. Consider physical security measures, access control, data storage and continuous training of specialized personnel.

Disadvantages

- Limited opportunities for customization
  A wide range of applications and services are available, but they have to be just right for the specific IT needs of your organization.
- Privacy considerations
  With the public cloud, it is not clear where (on which systems and in which countries) the data is located. Sometimes the government demands that organizations always keep certain data in-house.

All advantages and disadvantages in a row

Private cloud

When we use the virtualized IT environment exclusively for our own business, we speak of a private cloud. With private cloud, the applications and services reside with the cloud provider in a managed data center or in their own data center.
Just like for the public cloud. However, a private cloud is a fully shielded IT environment with its own servers for applications and data storage.

Your own IT department provides management and maintenance (or, if desired, a dedicated team from the cloud provider can do this).

Advantages

- Customized
  The applications and services are tailored to the needs of your organization.
- Privacy consideration
  You always know exactly where your data is stored. That is of crucial importance for financial institutions, for example. Laws and regulations require that they know exactly where the (customer) data is stored and how the security is arranged.

Disadvantages

- Higher investments
  Because of the customization involved in a private cloud, this solution may be more expensive than a public cloud. Consider additional investments for hardware, physical security and continuity. Higher costs for scaling up additional capacity should also be taken into consideration.

Hybrid cloud

The hybrid cloud is a combination of public and private clouds. The hybrid cloud offers you "the best of both worlds." You use the standard offerings of the public cloud, such as Microsoft Azure, Amazon Web Services or Google Cloud Platform.

In addition, you use custom solutions to comply with privacy legislation or to continue utilizing sector-specific or company-specific software. This handy combination ensures that the hybrid cloud is becoming more and more popular.

Advantages

- Financially attractive standard configurations with the speed and flexibility of the public cloud.
- Custom solutions for specific applications and systems like in the private cloud.

Disadvantages

- Higher investments than for the public cloud.
- Complexity of combining the public and private clouds.

Which type of cloud suits your organization?

The service models of the cloud

Once you have decided which form of the cloud best suits your organization, you must also decide to what extent you will outsource the management of the IT environment. "Everything as a Service," or XaaS, is at the heart of the cloud. This includes a number of service models:

Software as a Service SaaS

The most well-known 'as a Service' option is perhaps software (SaaS). Instead of purchasing software once, you pay for it according to use. Most SaaS solutions are used directly online without requiring a download or installation. SaaS also has the advantage that the vendor takes care of the management and storage of the application. These days there is a wide variety of applications to use via the internet: from office software (Microsoft Office 365, Salesforce.com) to accounting packages (AFAS Software, Exact), HR software (WorkDay) and ERP applications (SAP, Oracle).

House what where?

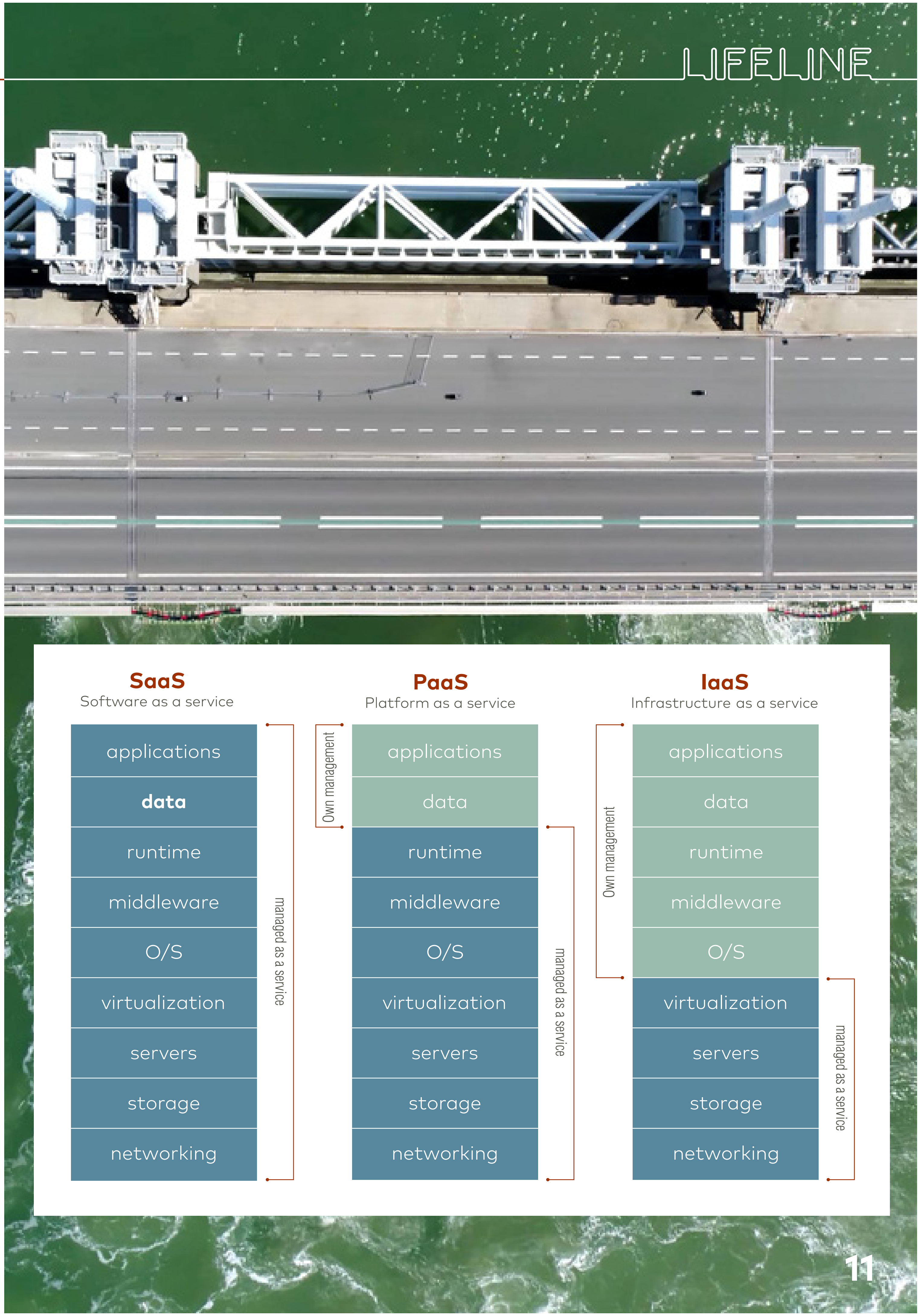
Platform as a Service PaaS

When organizations purchase a platform online on which they can develop custom applications, this is called Platform as a Service (PaaS). A PaaS platform consists of shared hardware for server and data storage, including the required virtualization software and operating systems. Maintenance and management are the responsibility of the cloud provider. Unlike SaaS, PaaS requires you to perform more administrator tasks yourself. This requires more knowledge and experience. The best-known PaaS providers are Amazon (EC2), Microsoft (Azure), Oracle and Google (App Engine).

Infrastructure as a Service IaaS

An IaaS solution provides your organization with a virtual hosting environment with control over data storage, network equipment and operating system, among other things. You only pay for what you actually use. A big advantage is that the extra capacity is available almost immediately and you do not have to invest in hardware or the location of a server yourself. Well-known IaaS parties are Amazon (AWS), Microsoft (Azure), Google Cloud Platform and Oracle (NetApp).

Moving to the cloud or expanding your cloud environment brings a number of challenges. What applications, data and platforms will you house where?



SaaS Software as a service		PaaS Platform as a service		IaaS Infrastructure as a service	
applications	managed as a service	applications	Own management	applications	Own management
data		data		data	
runtime		runtime	managed as a service	runtime	
middleware		middleware		middleware	
O/S		O/S		O/S	
virtualization		virtualization		virtualization	managed as a service
servers		servers		servers	
storage		storage		storage	
networking		networking		networking	

PROJECT ANN X: ADVANCED ARTIFICIAL NEURAL NETWORK FOR SPECIAL PURPO

3. Points to consider when migrating to the cloud

Now that you have a better picture of the cloud, it's time to take a good inventory of your own IT environment. Migrating to the cloud is a complex process. After all, different applications and systems need to be transferred.

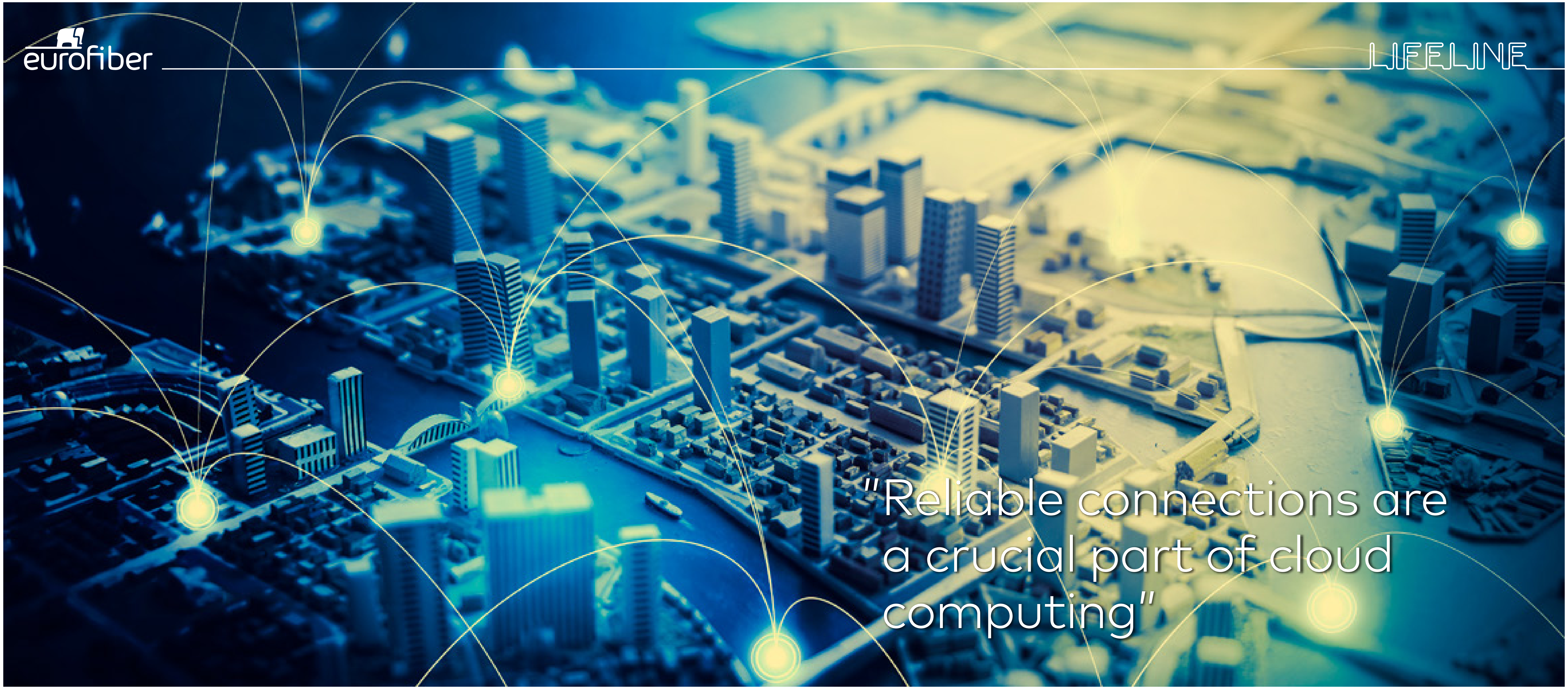
"Involve various colleagues in an inventory"

Think carefully in advance how you are going to organize the process. Which applications will go in the cloud? And will you be using multiple clouds? In that case you may have to deal with a variety of SaaS, PaaS and IaaS vendors. Will your department manage these parties itself or would you rather outsource this?

Make a complete inventory

When migrating to the cloud, you start by taking stock of your current IT environment. But beware: a good inventory goes beyond making a list of applications and systems. Your employees and the various departments use more IT solutions than the IT department often realizes. For example, consider cloud services they already use privately, such as Dropbox or Google Drive. Take steps to stop the proliferation of this shadow IT. You do this, for example, by clearly communicating who your preferred suppliers are. Involve your employees and departments in the inventory to understand the different expectations and interests at play. This is how you find out why your users are not using the IT solutions offered by the organization. Maybe it's even time for other vendors?

- How many branches and workstations do you currently have?
- What software and hardware do your organization's employees and departments use?
- Is there overlap between different applications and systems?
- Can the software also be purchased from the cloud?
- Should a number of applications (custom software or outdated business-critical packages) continue to run on your own server?
- Or are there good alternatives in the cloud?
- Who will manage your IT environment?
- Does your IT department have sufficient knowledge to migrate?
- How do you want to manage the chain?
- What is your policy on privacy and security?



"Reliable connections are a crucial part of cloud computing"

Connections with the cloud

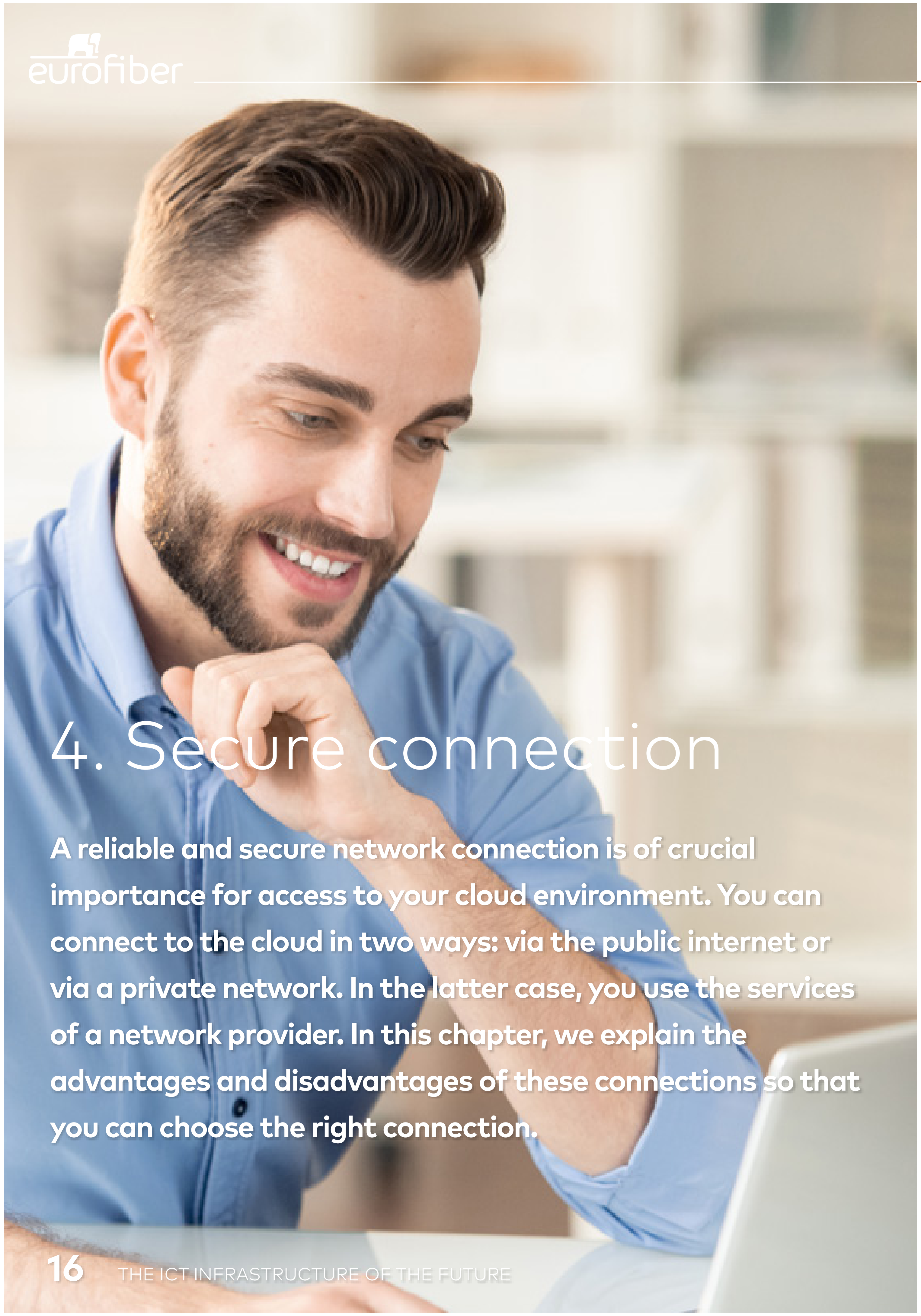
When you take inventory, it's also time to take a critical look at the current infrastructure. Reliable connections are a crucial part of the cloud, so take a close look at your internet and network connections. Will your bandwidth suffice in practice in the future?

Exit strategy

The last point to consider is that of a successful exit strategy. If you want to switch from one cloud provider to another, you will need to arrange this well in advance. For example, by including in the contract with the cloud provider that company data can be transferred to a new party easily and quickly without incurring additional costs.

Consider:

- How many separate internet and network connections are there?
- Can you always access your data?
- Has redundancy been taken into account?
- Does the network provider also offer the necessary guarantees for the continuity of its services?
- Does the network provider have certifications that guarantee quality?
- In terms of connections, what are the recommendations of the cloud providers with regard to bandwidth and quality requirements?
- How will you organize connectivity to these platforms or applications?
- How important are they for the continuity of your organization?
- How do you guarantee the security of your IT environment?



4. Secure connection

A reliable and secure network connection is of crucial importance for access to your cloud environment. You can connect to the cloud in two ways: via the public internet or via a private network. In the latter case, you use the services of a network provider. In this chapter, we explain the advantages and disadvantages of these connections so that you can choose the right connection.

"Should you choose a public or a private network?"

Via the public network

The public internet seems like the easiest way for organizations to connect to the cloud. Unfortunately, there are quite a few drawbacks to this solution:

- There is no control over the various "intermediate stations" over which corporate data and applications are sent. A true Quality of Service (QoS) on the connection cannot be issued with the public internet.
- Scalability is limited. Quickly scaling up in the event of peaks in the use of cloud applications is not possible. Therefore, you need a reasonable bandwidth to be able to meet the required extra capacity.
- The security is not watertight. If you want to establish a secure cloud connection, you will have to invest extra funds in a more secure connection.
- Then you will have to connect the network to the cloud provider of your choice.

Via a private network

When you choose a private network for accessing the cloud, your data traffic travels through a private connection over a closed network. In effect, the connection with the cloud becomes part of your corporate network. There are two possible approaches. You can set up a private network completely by yourself or use a network provider.
You need high-quality broadband connections in both cases.

When you set it up yourself, extensive expertise and specialized knowledge is required. Connections must be established, rack space rented and set up in data centers where the various cloud platforms run. Knowledge about the different network layers, BGP protocols and IP routing to connect to the cloud platforms is also required. After that, you can start building and setting up the cloud environment.

The alternative is to use the services of a network provider for an IaaS connectivity solution. The network provider gives you private connections to the data centers of the various cloud providers over their pre-configured infrastructure. This offers you a number of benefits:

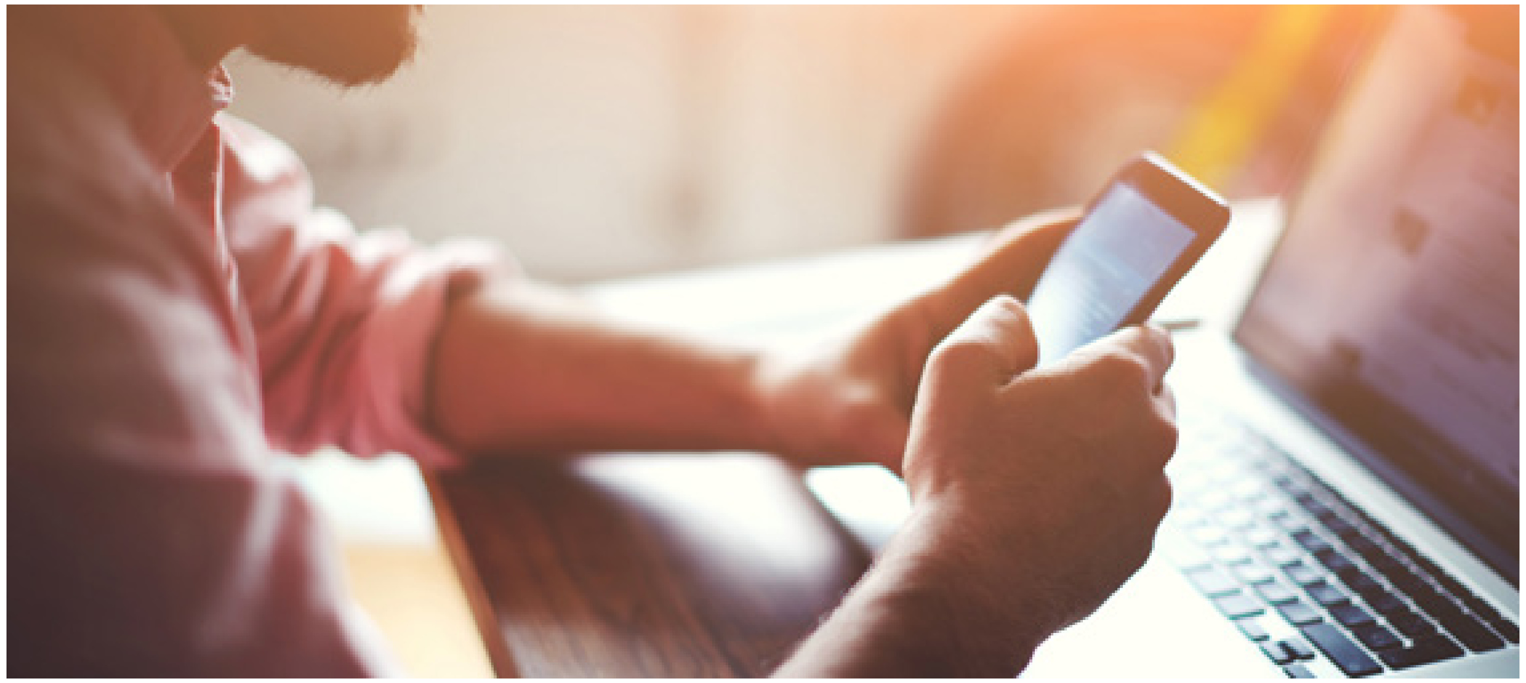
- Good access security to your applications and data in the cloud. Namely, the network is set up based on private Ethernet or IP VPN connections and is completely separated from the public internet. (read more about VPN in the box on this page)
- A one-to-one relationship with the network provider, with a Service Level Agreement (SLA) specific to the contracted service.
- Some network providers offer end-to-end connectivity through their network to connected cloud providers, completely set up on a cloud exchange or direct links to the various cloud providers. This complete solution offers redundancy to the cloud, very high availability and, not unimportant, a service at relatively low cost. The only thing you have to take care of is setting up your cloud environment. These solutions fully fit the cloud model of unburdening, scalability and flexibility. And you do not need to have any specialist network knowledge to link directly with cloud providers or to set up a data center infrastructure.

What is VPN?

VPN stands for Virtual Private Network: a virtual data network between locations that is separate from the public internet. With VPN connections, you create a closed organizational network between your headquarters, branches and data centers. The network is easy to expand and stimulates employees to work efficiently.

The advantages of a VPN

- You can transport multiple services over your VPN connection, such as internet, telephony and video. By also opening up your data centers via the network, it is possible to offer applications and platforms centrally.
- For your organizational network, you can determine the bandwidth requirements for each connection. This allows you to be flexible at peak times.
- You can connect your headquarters, branch offices and internal or external data centers via single or redundant connections. The importance of the location determines what kind of connection you need.



"Future-proof solutions"

5. Security policy

The cloud and the connections to it require a modern and future-proof security policy. A policy that protects all new connections and storage capabilities from cybercriminals. The consequences of a cyberattack can be a disaster for your organization. How do you ensure that you set up your organization to be as secure as possible?

"Now, more than ever, it's safety before everything"

The financial consequences of a cyberattack

The moment a cybercriminal infiltrates your organization, the consequences are dire. Cybersecurity specialist Kaspersky has researched that the costs following a cyberattack to businesses range from $120,000 to as much as $1.23 million*.

Some of those costs are directly related to the aftermath of the cyberattack, such as plugging the leak and hiring security experts. The biggest costs, however, come from lost revenue and reputational damage. Your organization will be portrayed in a negative light. And that's not all. You may receive claims from third parties. In addition, you could be fined a considerable amount of money by the central government. In the European Union, the General Data Protection Regulation requires you to report a data breach within 72 hours. If you fail to do so, or do so too late, the fine can be as high as €20 million, or 4 percent of the company's global annual turnover**.

What the cost to your organization will be depends very much on the type and size of your organization and also the form of the cyberattack. We recommend that you seek advice from a security specialist in advance.

Security in the cloud

When you purchase a cloud service, many cybersecurity measures are the responsibility of the cloud provider. They take security very seriously and invest heavily in it. These investments range from physical security, access control and data storage to continuous training of specialized personnel.

In doing so, many cloud providers go further than an organization itself could. To reduce the risk of a cyberattack, you should also take measures yourself, such as setting up a Cyber Threat Management platform or purchasing a Security Operations Service. Make sure you have an appropriate antivirus system on all your devices and have updates done regularly. And, perhaps most importantly, make sure your employees know how to work safely.

Teach them what is and is not allowed when it comes to access to applications and data and teach them how to set strong passwords. For example, organize regular awareness sessions in which they learn to deal with the risks of cybercrime.

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

Connections neglected aspect of cybersecurity

The connection to the cloud is a neglected element in security. Yet it is an essential link: all applications and data run through the connection with the cloud provider. This is the best entryway for cybercriminals to strike.

Network monitoring

Therefore, continuously keep an eye on your connections through monitoring.
This allows you to detect disruptions in the network immediately. In the case of Ethernet and IP VPN connections, this monitoring is twofold: the supplier has an overview of his own network and you, the customer, have an overview of the entire setup, including your own network and the equipment it contains. If failures occur, it is easy to determine whether the failure is a result of (planned) work or whether something else is going on. All network equipment comes with monitoring tools that measure latency, retransmissions and bit errors, among other things.

Actively manage your network components and ports so that when latency changes and signal interruptions occur, you see alarm bells go off immediately. These are indications that potentially unwanted devices have been placed in the network. The major cloud providers have now developed solutions for direct and secure access over a network connection.

"Eurofiber's Secure Cloud Connect"

In order to be versatile and flexible as an organization, you are going to work from the cloud more often. With Secure Cloud Connect, you'll always have secure and immediate access to multiple cloud platforms. With this complete end-to-end solution, you get instant access to the platforms of your choice over a secure private network.

6. Eurofiber's Secure Cloud Connect

In order to be versatile and flexible as an organization, you are going to work from the cloud more often. With Secure Cloud Connect, you'll always have secure and immediate access to multiple cloud platforms. With this complete end-to-end solution, you get instant access to the platforms of your choice over a secure private network.

Efficient total solution

We connect your organization to your cloud providers via a virtual private network (VPN), with the network completely separated from the public internet. You also gain direct access to the platform of your choice through our cloud links.

Eurofiber delivers an end-to-end service from your office and/or data center location to public cloud service providers such as: Microsoft Azure, Microsoft Office 365, Amazon Web Services (AWS) and Google Cloud Platform.

Other cloud platforms are available upon request. With Secure Cloud Connect, you only manage your applications in the cloud; we take care of the rest for you.

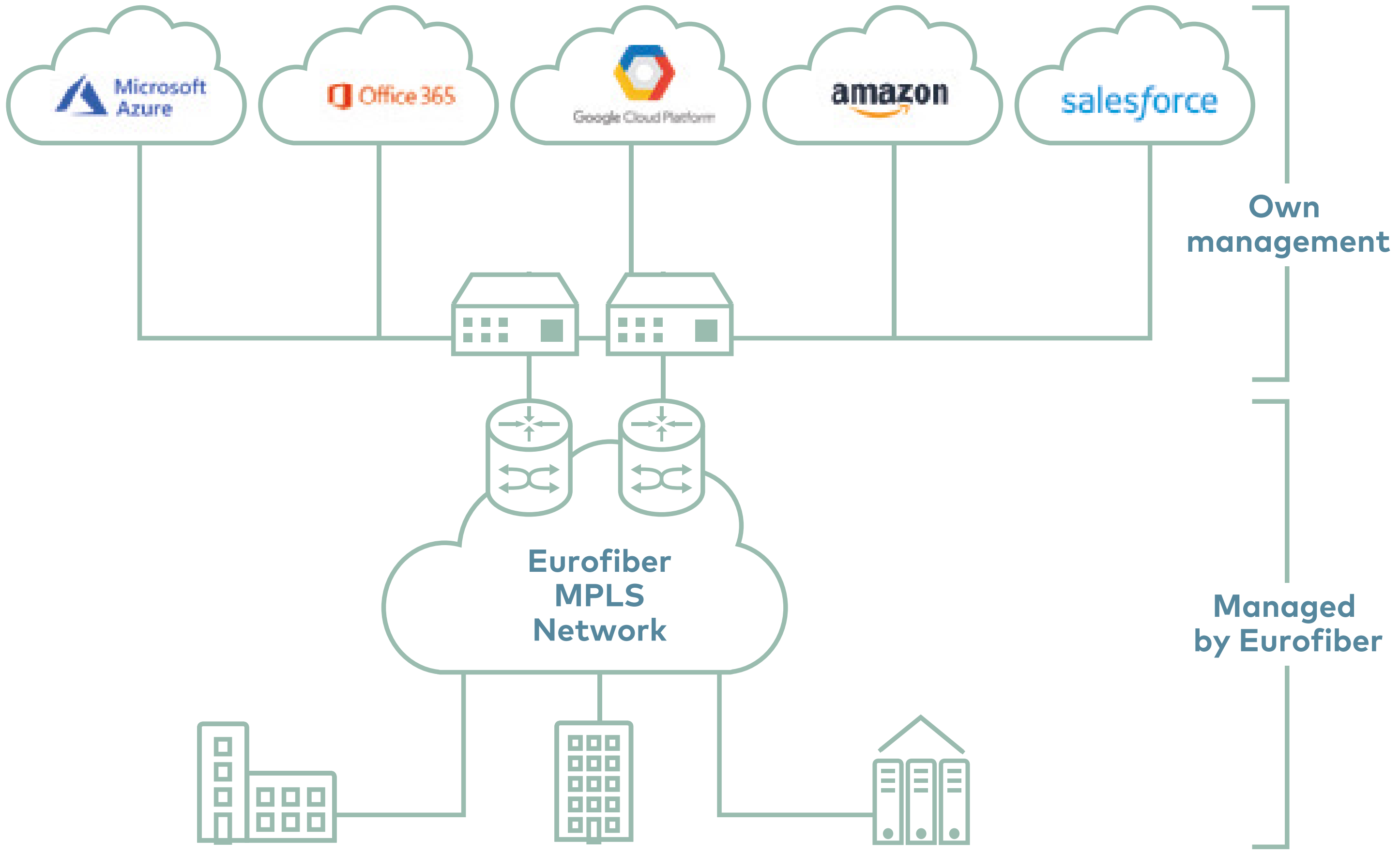
Customized for your organization

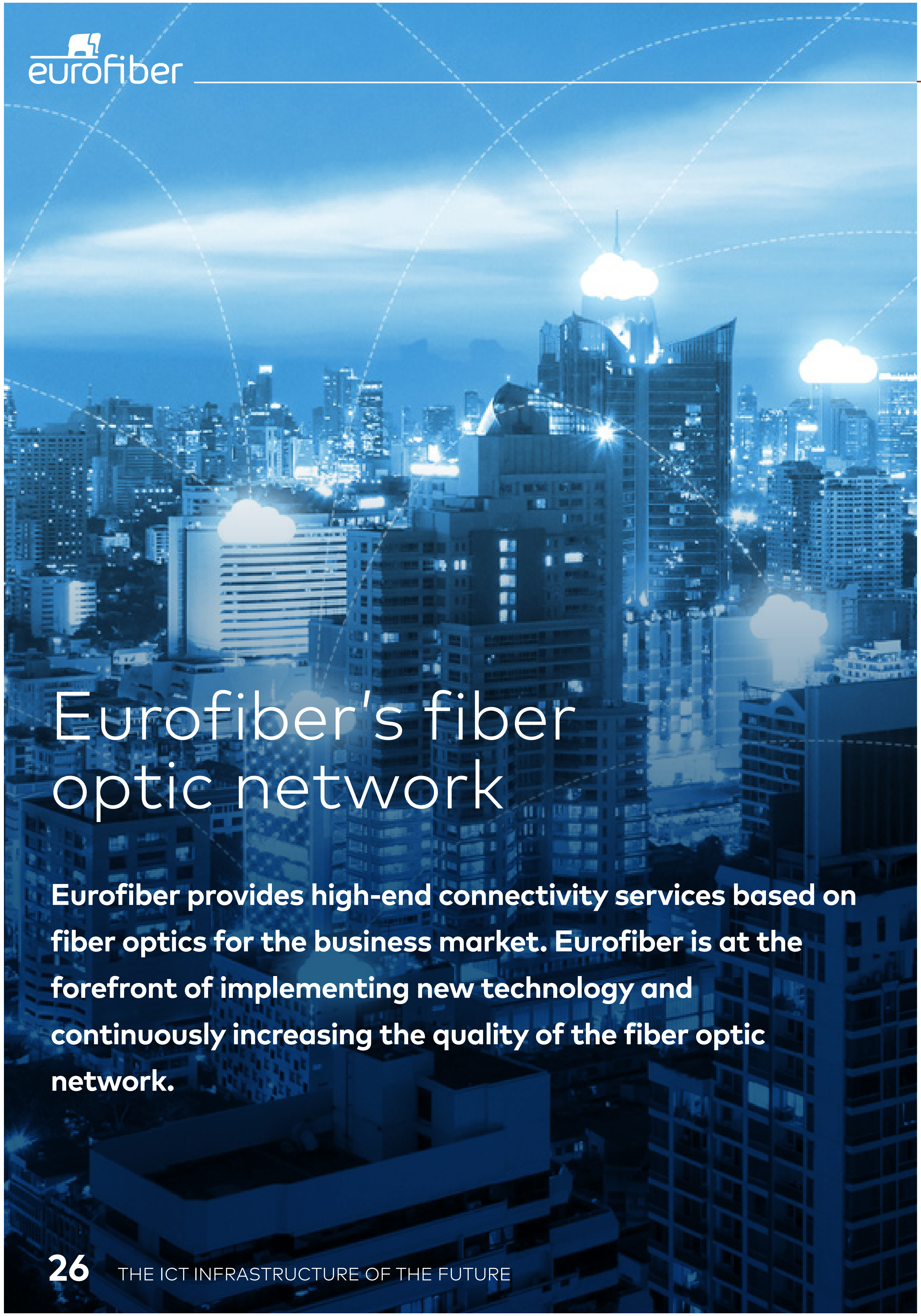
We always offer you a complete solution that is optimally suited to your organization's situation. We are happy to advise you on setting up your network: internet, VPN network between your main and secondary offices, data centers and integration of cloud service providers.

You can flexibly set up your network per location according to bandwidth, service level and single or redundant configuration. Secure Cloud Connect supports all bandwidths of the various cloud service providers from 50 Mb/s to 10 Gb/s, both single and redundant connections.

Optimal availability and support

To offer your organization reliable access to your cloud providers, we always deliver Secure Cloud Connect over Eurofiber's fiber optic infrastructure and the Eurofiber private layer-2 network. You can also count on 24/7 support from our Network Monitoring Center (NMC).





Eurofiber's fiber optic network

Eurofiber provides high-end connectivity services based on fiber optics for the business market. Eurofiber is at the forefront of implementing new technology and continuously increasing the quality of the fiber optic network.

Eurofiber

Eurofiber has been operating high-quality digital open infrastructure since 2000. With our own fiber optic network and data centers, we offer companies, government bodies and non-profit organizations a future-proof, smart and open infrastructure. Customers have the freedom to choose for themselves the services, applications and providers they need. This enables them to fully exploit the innovation potential in digitization.

In addition to our extensive fiber optic network in the Netherlands and Belgium and our own data centers in the Netherlands, we also offer solutions for interconnectivity between almost all high-quality carrier-neutral data centers in the Benelux. Eurofiber is thus laying the foundation for the digital society.

Flexible and scalable

Our open network gives your organization complete freedom and flexibility. You have the freedom to choose the services, applications and providers that you need. Eurofiber also offers managed services based on the fiber optic network, such as WDM, Ethernet and internet.

Safe underground network

Eurofiber's network lies underground at a depth of 60 centimeters. Work on our network is carried out using certified processes, which we monitor continuously and test annually. We work with certified employees and contractors. A Remote Fiber Test System (RFTS) has been installed on the network; it continuously monitors the availability of the infrastructure. In the event of unexpected cable damage due to excavation work, for example, the RFTS can measure exactly where the damage is located. To prevent disruptions for our customers, regular preventive maintenance is carried out to guarantee network quality.

Extensive experience in the public sector

High availability

The availability of Eurofiber's fiber optic network is at least 99.9%. If you opt for a fully separated, second fiber optic route (redundancy), this availability is at least 99.98%. If you have two separate fiber optic connections, we guarantee that we will never work on both connections at the same time. We will inform you, as a customer, when work is planned on the network.

Network Monitoring Center

You can count on the 24/7 support of the experts at the Eurofiber Network Monitoring Center.

Guaranteed repair time

The geographically defined Eurofiber fiber optic network, combined with the active monitoring of the Network Monitoring Center, ensures that the guaranteed repair time on fiber optic connections is a maximum of 8 hours. For active services this is a maximum of 4 hours.

Available in 92% of the data centers in the Benelux

Eurofiber's fiber optic network is available in a large number of data centers in the Benelux. With the additional Data Center Services from our sister company Dataplace, which has modern, Tier 3 data centers in the regions Amsterdam, Rotterdam, Utrecht, Arnhem and Brabant, we support you with high-quality colocation solutions for the secure housing of your business-critical information and systems.

Guarantees

Eurofiber provides connectivity on the basis of a Service Level Agreement. This determines exactly what performance, quality level and guarantees you can expect from us. Clear agreements, so you always know where you stand.

For more information, please contact us:
Belgicastraat 5, bus 7, Building Fountainplaza 504, 1930 Zaventem
t +32 (0)2 307 12 00, info@eurofiber.be
www.eurofiber.be

Eurofiber. Lifeline for the digital society

eurofiber