Virgin media O2 Business

Now and Next -

Connect

How connectivity can help businesses now and looking ahead to the future

Why it’s time to think about connectivity

Whether it’s working from home, on the move, or in the office, reliable connectivity is the bedrock of modern productivity.

When connectivity is poor, people waste time. Waiting for data to process. Dialling back into calls. Waiting in the phone queue to speak to IT support. As well as a drain on productivity, it’s also hugely frustrating. According to a study by Adobe, 49% of employees would consider quitting their job due to poor technology experiences[2].

Connectivity is also changing. Many organisations have a dedicated physical WAN, like IPVPN or MPLS. But the accelerating use of cloud apps and tools as well as wider digital transformation initiatives, means there is a drive to change the underlying connectivity infrastructure. Of course, your employees and customers don’t really care what that infrastructure looks like as long as it works.

We all rely on connectivity but there are lots of options to consider. It means that businesses need to think about what connectivity they need now and what they will need in the future. Especially if they want to keep their employees productive, secure and enable business growth in the cloud.

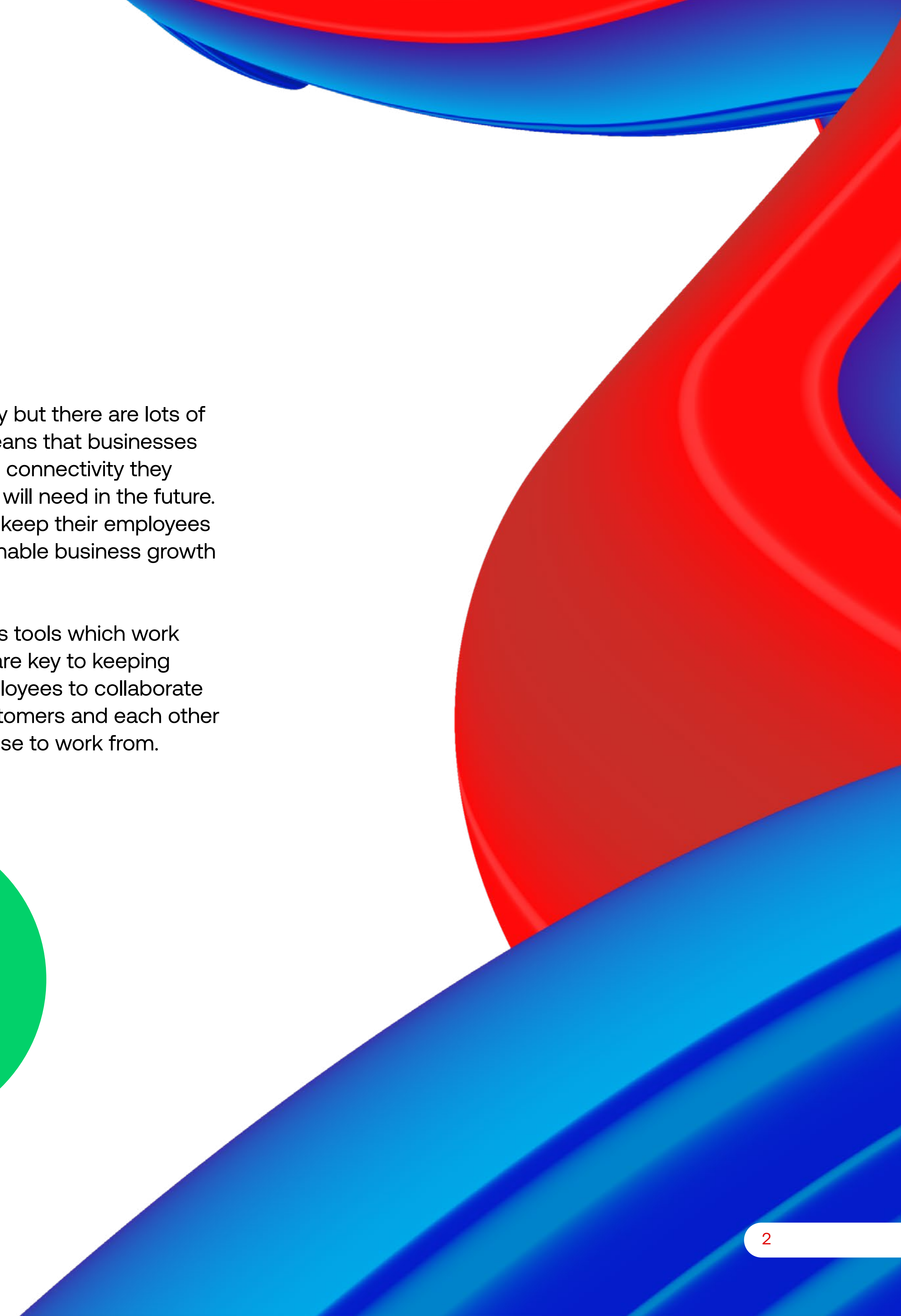
Powerful communications tools which work over mobile and on-site are key to keeping connected, allowing employees to collaborate effortlessly with your customers and each other 24/7, wherever they choose to work from.

93%

of businesses are investing to support a digital-ready workplace and hybrid work environment[1]

82%

of IT buyers intend to leverage MSPs in 2022 – a new record high[1]



[1] TechTarget, 2022 IT Priorities, 2021
[2] Adobe 2021

Next generation connectivity looks beyond traditional WAN

Up to now, traditional WAN has been the centre of connectivity, but those days are coming to an end.

There are now options such as SD-WAN, hybrid with MPLS or through-internet enabled by building blocks such as Ethernet and fibre. Blending some of these forms of connectivity infrastructure can give you a robust, reliable, high performing and cost-effective network.

Cellular connectivity – whether 4G or 5G – should also be a key consideration for businesses connectivity infrastructure. It's particularly useful in sites that are difficult to access with traditional fixed connectivity.

But it's also key where rapid set-up of sites is required, such as for retail stores or construction sites. Or for new connectivity requirements like disparate IoT sensors.

There is also huge potential for businesses to utilise private cellular networks. These are custom-built networks designed to provide dedicated, secure connectivity across their sites.

To-date, these have mostly relied on 4G connectivity. But with the introduction of 5G, there are opportunities to develop new use cases thanks to the higher speeds and far lower latency compared to 4G.

These next-gen features are critical for creating value at scale from applications like autonomous vehicles, robotics, AI and automation. In turn, the rewards from such investments will be increases in productivity, operational efficiency, and better health and safety practices.

As with the roll out of any new connectivity technology – whether that is SD-WAN or 4G IoT or 5G private networks – the promised benefits are intrinsically dependent on the degree to which that connectivity is secure. Indeed, connectivity is king.

How things could change back at the office

Despite the shift towards hybrid or remote working, the office and physical workplace must still be considered. In particular, how might these new ways of working put a burden on your legacy office infrastructure?

Many employees have more devices now than they when they ‘left’ the office at the start of the global pandemic. They’re calling Teams, Webex or Zoom more than ever than they worked before, including communicating with their colleagues working remotely.

This has worked fine from home, where traffic routes straight through the internet and the quality of the session is generally good. It also doesn’t create an overhead for the LAN. But can the traditional connectivity infrastructure in your office cope with the new demands brought around by the changes in how people use technology?

Rethinking how people can connect at work could involve investing in higher-bandwidth WiFi. Or reconfiguring WAPs that were set up pre-pandemic and now need to reflect a change in working practices, such as the increase in hybrid working, collaboration via video calls and people using multiple devices at work.

Gaining more control over network services: how can your service provider help?

Service providers have always had more in their locker than just the core connectivity infrastructure.

Service providers have provided many of the managed services that made that connectivity work for individual business requirements. Now, an increasing number of organisations are investigating ways to gain more visibility or control over their network services.

This need can be addressed – in part – by moving from legacy networks such as MPLS to SD-WAN, which offers visibility and control at the application layer. Being ‘software defined’, it also promises the ability to make swift changes to service.

Deciding on the right level of control over the network is still highly dependent on what the organisation needs.

If you opt for a fully managed service from your service provider, it offers an increased level of security and peace of mind knowing that your network is in safe hands. There is, of course, the associated management costs as well as the need to live with the provider’s timescales for MACs.

In some cases, it may be preferable to take back some level of control or acquire the ability to make changes yourselves. If this is your direction of travel and you want to look after certain elements ‘in-house’, there are some key considerations to discuss with your service provider.

Eight areas to discuss with your service provider →

Eight areas to discuss with your service provider

1. Establish clarity: Define what will be managed in-house and what will be managed by the service provider, with clear roles and responsibilities.

2. Add value: Consider the best ways any agreed approach can add value. For example, perhaps your service provider can take away the more labour-intensive tasks to free up your internal teams for other important projects.

3. Agree the small print: Changing services provided will involve amending SLAs and T&Cs to ensure both parties are protected, along with along with adjusted pricing and potentially a rate card for agreed activities.

4. Focus on processes: Agree methodologies and processes such as how will you deal with different situations, who will resolve them and what with the SLAs look like. Make sure you also agree roll-back processes in the event anything goes wrong.

5. Assess in-house skills: Assess whether you have the necessary in-house skills to support the day-to-day management of the network. The savings from not paying for a fully managed service could soon be wiped out by the costs and resources required to manage tasks and retain those skills.

6. Ask about training: Ask if your service provider could help to keep your people up to date with their training and consider joint training initiatives that build on the understanding on both sides of the partnership.

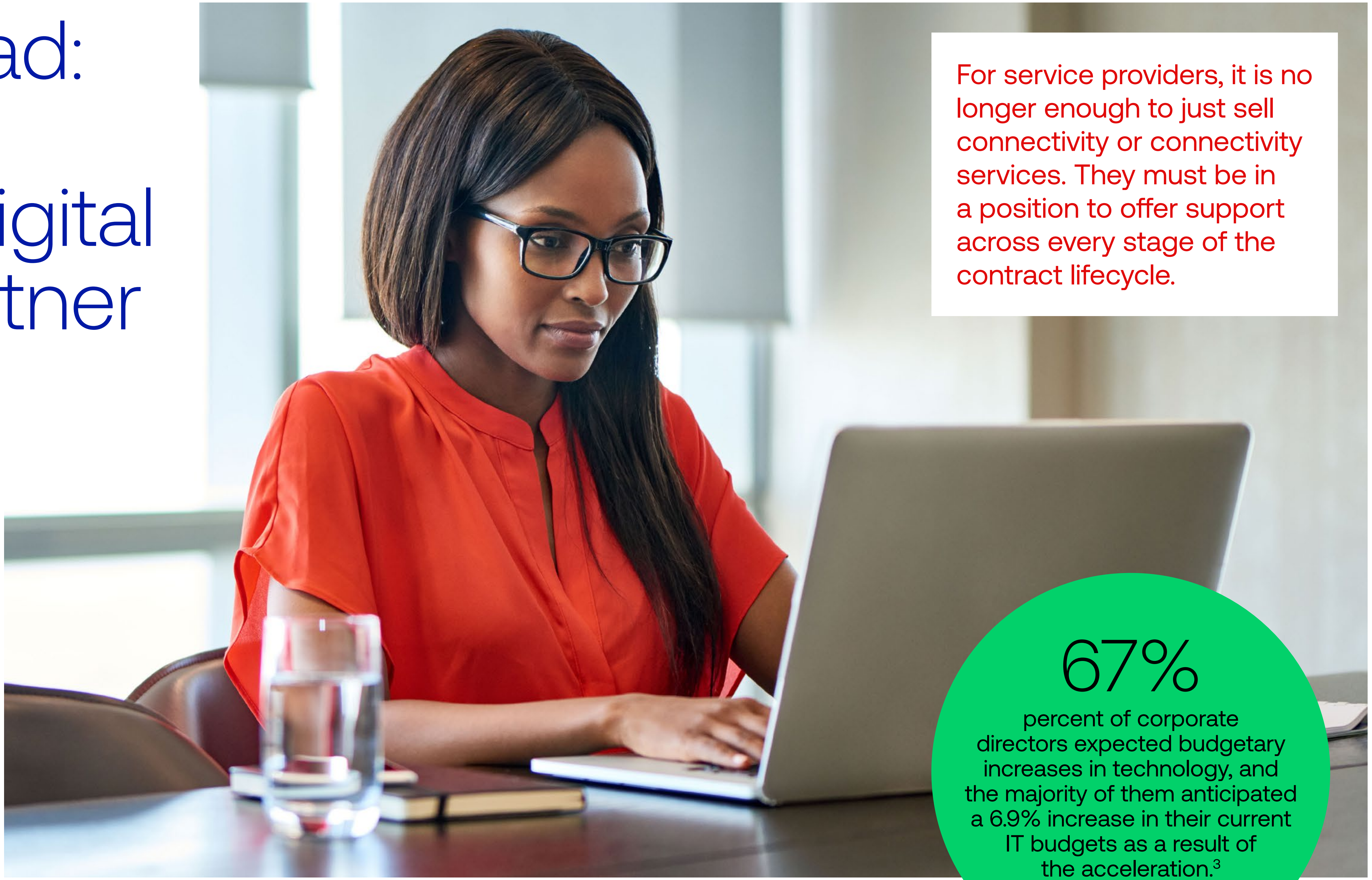
7. Get the right platforms and access: Ensure you've got the right platforms in place and that the right people have the right level of access to those platforms.

8. Invest in change control: Introduce a change control board for both parties to participate in.

Looking ahead: from service provider to digital business partner

Plenty of organisations made rapid investments at the beginning of the global pandemic to get people set up and able to work from home quickly. However, uncertainty about the best ways of working moving forwards means that some of those organisations are delaying investment decisions and rolling over current contracts while they assess their options.

It's important to weigh up the cost/benefit of investment compared with the cost/benefit of doing nothing. Those looking for longer-term value and additional support in making the right investment decisions, are choosing to view their service provider as a support partner and trusted adviser rather than just a supplier.



For service providers, it is no longer enough to just sell connectivity or connectivity services. They must be in a position to offer support across every stage of the contract lifecycle.

67%

percent of corporate directors expected budgetary increases in technology, and the majority of them anticipated a 6.9% increase in their current IT budgets as a result of the acceleration.[3]

[3] Gartner: COVID-19 accelerates digital strategy initiatives

Seven ways service providers can support the contract lifecycle

1 Helping to build the business case and demonstrating the long-term value and return on investment the service will provide

2 Running a proof of concept/proof of value to demonstrate the business case and help to convince senior stakeholders

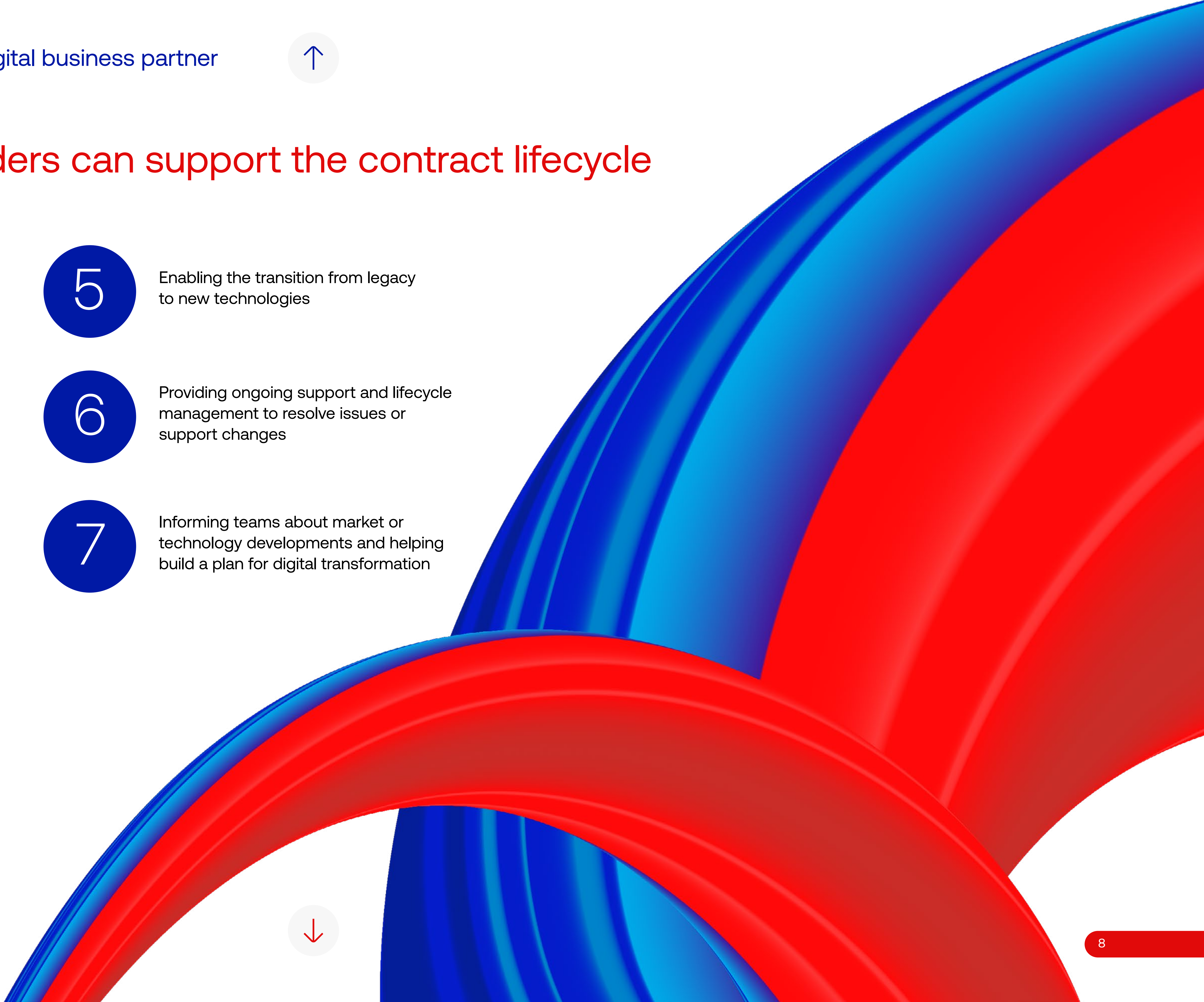
3 Supporting the early-life of the service to ensure maximum user adoption and better ROI

4 Delivering training or guidance to support users and helping with internal comms

5 Enabling the transition from legacy to new technologies

6 Providing ongoing support and lifecycle management to resolve issues or support changes

7 Informing teams about market or technology developments and helping build a plan for digital transformation



AI and automation: the connectivity of tomorrow

Organisations that are looking ahead expect a service provider to remain relevant in order to become a truly trusted partner.

One area that service providers can demonstrate this is through advice on connectivity and beyond. Since connectivity, collaboration and security are all interlinked, it is rare that a decision in one area does not affect what happens somewhere else. The role of a trusted advisor is further enhanced by advice on what investments the organisation should be prepared to make in the coming months and years.

The connectivity networks of the future will use advanced algorithms and smart analytics driven by machine learning and AI. They will use these technologies to self-triage, self-heal and self-optimise, ensuring critical traffic is services and applications are optimised.

AI will automatically monitor network data using real-time insights into the users, devices and applications, speeding up troubleshooting and ensuring optimal network performance.

83%

of organisations are investing in automation in 2022[4]

[4] TechTarget, 2022 IT Priorities, 2021

By using AI in this way, service providers should be well-placed to bring together experience in managing the wider network with your own pool of knowledge to add value. For example, enabling your own network to self-manage and optimise via automated processes will free up your IT team to address real business problems or facilitate internal innovation.

This also opens the door for lower operating costs by reducing the internal resources required for network management.

As the use of automation improves and expands into most areas of connectivity, security will become critically important. So, your organisation will need to liaise with its service provider to coordinate sophisticated approaches to potential cyber threats, such as integrating the threat-hunting skills of the provider's SOC analysts.

1 in 6

of organisations will launch first-time automation projects during the coming year[5]

[5] TechTarget, 2022 IT Priorities, 2021

Staying cyber secure

As the use of automation improves and expands into most areas of connectivity, security will become critically important. With workers using a wider range of devices, network and endpoint security should adapt to changing habits and workstyles. AI-powered, cloud-based endpoint security can keep you ahead of real-time threats, following the user rather than the network and applying a security blueprint anywhere on any device, enforcing a consistent security policy at all times.

Your organisation will need to liaise with its service provider to coordinate sophisticated approaches to potential cyber threats, such as integrating the threat-hunting skills of the provider's SOC analysts.

Want to talk?

By working with you, we can help you and your people achieve more – right now and well into the future. We'll go beyond being just your connectivity provider. Instead, we'll respond to what your organisation needs as your digital business partner.

Talk to your account manager today or call us on **0800 955 5590**

Business

For more insight into how your business can leverage technology to solve problems now and into the future, discover more in the Now and Next series:

Now and Next – Empower

Now and Next – Protect