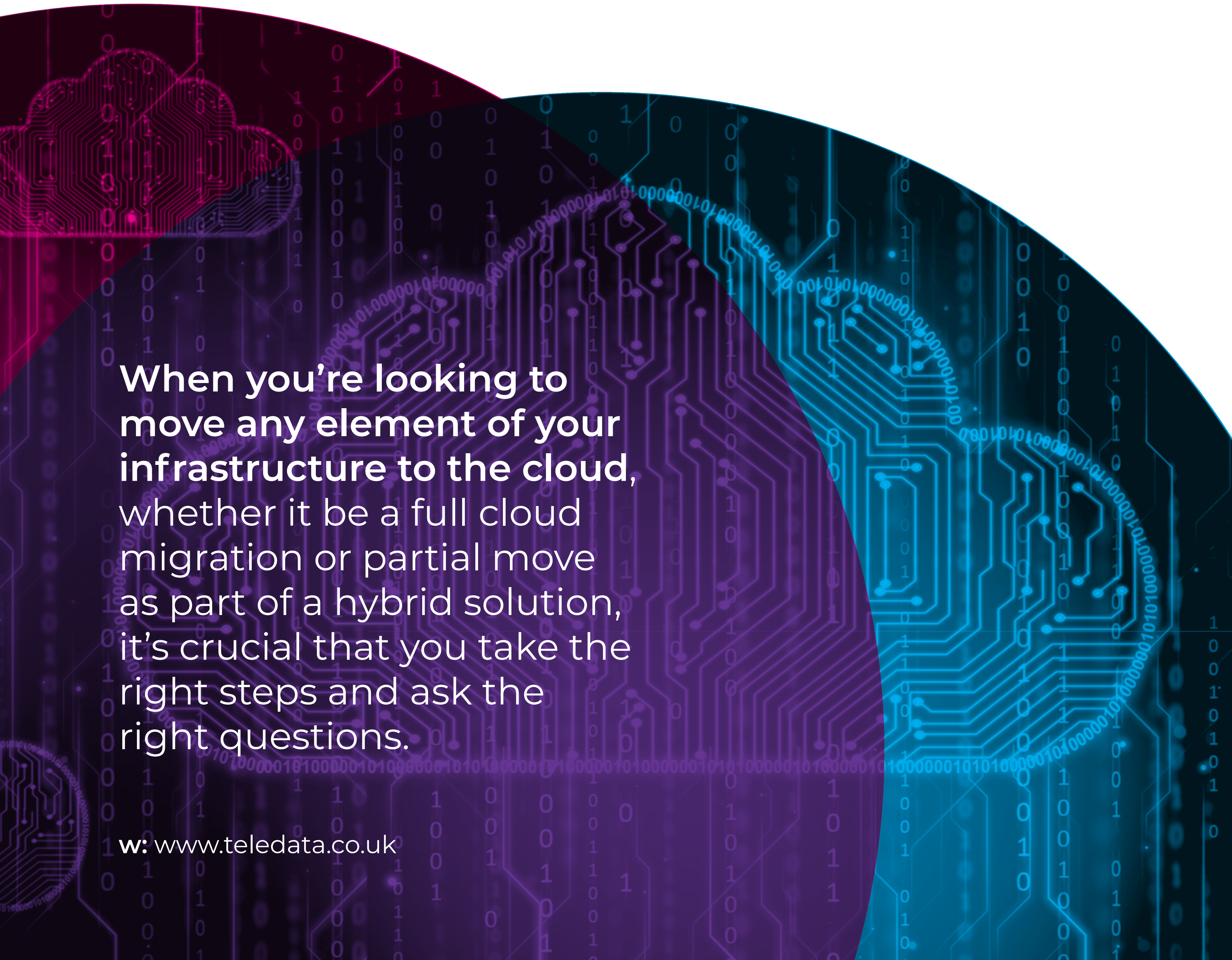
teledata™
people and technology together

Your cloud security guide



When you're looking to move any element of your infrastructure to the cloud, whether it be a full cloud migration or partial move as part of a hybrid solution, it's crucial that you take the right steps and ask the right questions.

w: www.teledata.co.uk

Welcome to Teledata

We're a Tier 3 data centre facility in Manchester, located right at the heart of one of the Manchester Airport City Enterprise Zones.

We're ISO27001 accredited and we provide premium colocation, cloud hosting and data centre services to businesses across the country. We're proud to be one of the most secure, resilient and well-connected data centres in the UK. In fact, our Security and Operations Control Centre (SOC) means that we're the only data centre globally, with an NSI Gold Approved BS5979 security centre on-site.

Bringing people and technology together...

Delivering the highest levels of service and support, we put people at the heart of our technology with solutions that are designed to optimise your business performance, empower your teams and help you to grow. Providing our network of clients with best-in-class hosting solutions, we can truly help to drive your business forward.

Our building, our builds, our people

We're proud to be Manchester's only premium independent data centre. We own the buildings that the servers are housed in, we built the data centres to top specification, and our dedicated support team is based right here too, looking after a network of clients across the globe.

Our people, your team

We bring people and technology together, and you can bank on our team of passionate technical experts to support you every step of the way.

All of our engineers are VMware® certified, SC cleared and background checked, and our customer support team is based right here on-site at Delta House in Manchester. In fact, the people you'll be chatting to about your everyday questions and queries are the people that built our data centre from the ground up, because we think there's nobody better to advise you, than them.

We'd love to see you...

Why not pop in for a tour of our facility? Visit our website at **www.teledata.co.uk** or call **0161 498 1200** for details.

Contents

1. Introduction 1

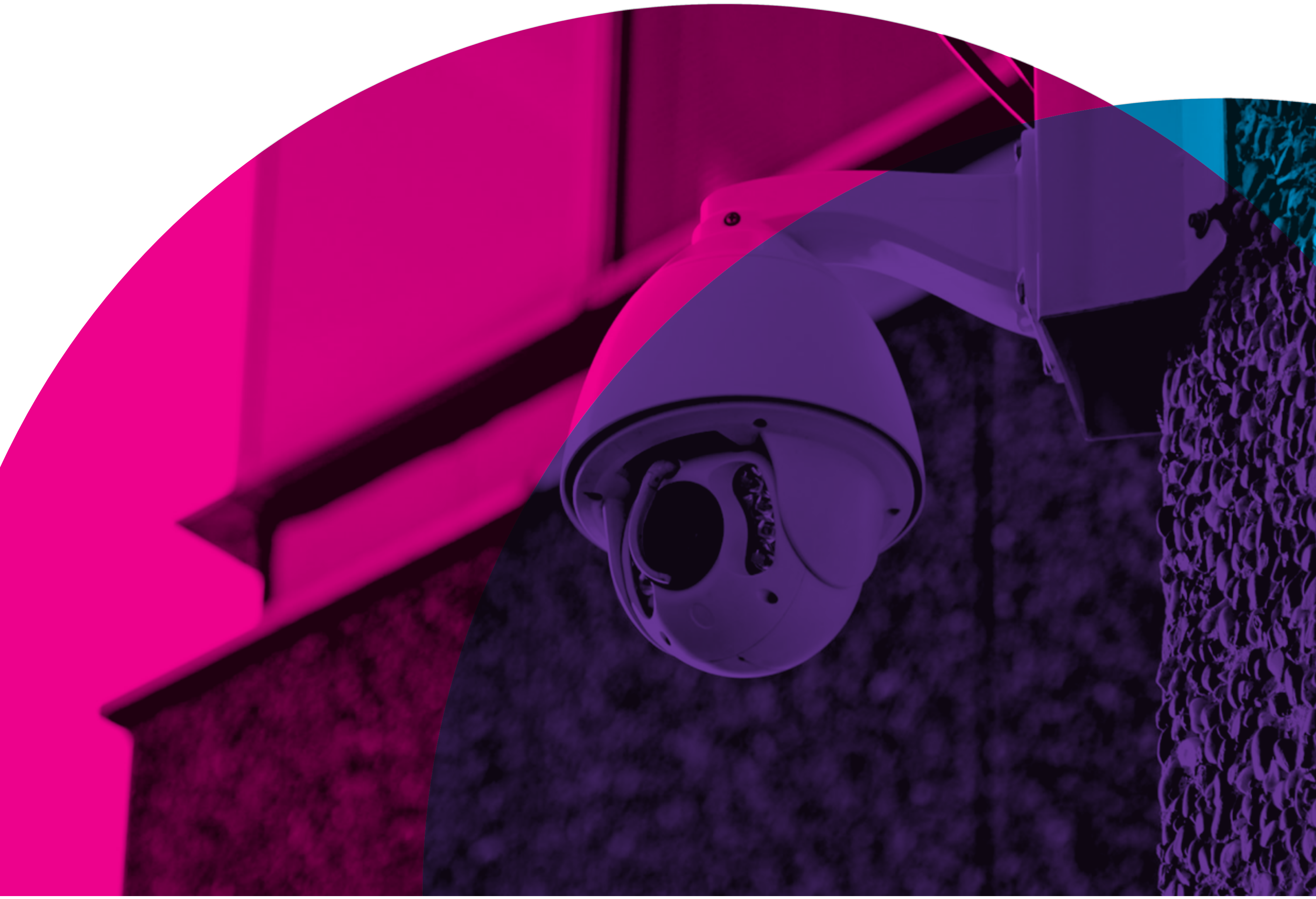
2. Risk assessment 2

3. Encryption 3

4. Physical security 4

5. Beware human error 5

6. Conclusion 6



Introduction

Despite the fact that 98% of businesses now use the cloud — according to Flexera 2020 State of the Cloud Report — cloud security is still a hot, and very important topic of conversation.

When you're looking to move any element of your infrastructure to the cloud, whether it be a full cloud migration or partial move as part of a hybrid solution, it's crucial that you take the right steps and ask the right questions to ensure that the security of your solution meets your compliance requirements.

> Remember, with the cloud you're putting your data on networks that you don't control, so you need to have complete trust in your cloud provider. It should be a true partnership.

And it's not just your cloud storage solutions that need to be secure. Data in-transit can be vulnerable to attack. As with most situations, the risks can be alleviated if the correct measures are put in place. Remember, with the cloud you're putting your data on networks that you don't control, so you need to have complete trust in your cloud provider. It should be a true partnership.

Risk assessment

Extensive cloud computing risk assessments will help businesses to make informed decisions before they go ahead with a cloud migration.

The type of solution and the amount of risk that a business can potentially open itself up to, will depend on the sort of data that is handled and the compliance regulations governing a business's industry. A company that handles particularly sensitive data or IP, for example, would likely need to maximise security, whereas a business that is trafficking less sensitive data might be in a position to accept a bit more risk, and with that, pay a bit less for its solution.

> A risk assessment matrix will help you to cover important elements such as the physical security of the data centre housing your cloud platform and data...

A cloud computing risk assessment matrix is a good starting point, such as Cloud Security Alliance's Cloud Controls Matrix. A matrix will help you to cover important elements such as the physical security of the data centre housing your cloud platform and data, cyber security and contingencies for continuation of service in the event of power outages and other disaster recovery options.

Encryption

As mentioned previously, your data can be at risk in-transit as well as at-rest, so you should consider pre-encrypting your data so that even if sensitive data is stolen during transit, it will not be usable without the key.

There are various different types of cloud encryption, but basically data is encoded as it travels to and from cloud-based applications and storage to authorised users, as well as being encrypted on cloud-based storage devices. Encryption can be highly effective in protecting sensitive data in the cloud in the event of a breach, and can also help meet new data sovereignty requirements.

Physical security

We've talked briefly about the physical security of the data centres housing your data, but this is critical. All too often, businesses migrate to a cloud provider without ever asking the question — where will my data actually be?

Some providers will have failover systems in place which may mean that your data could end up in any one of several data centres across the country, or even around the world. And while this might not be an issue for most businesses, those that are governed by industry bodies which dictate that data must not leave the UK, will face problems if their data fails over and across borders — particularly with Brexit in mind.

Any good cloud provider should be able to offer you a data centre tour of the facility where your data will be housed. Even if they don't own the data centres, enabling you to see for yourself the security protocols in place, and ask any relevant questions.

Supporting information

We have two other whitepapers available that might help you in this area:

- **10 questions you should be asking your cloud provider**
- **The data centre services buyer's guide**

Beware human error

Despite all these security measures, the weakest link in any IT infrastructure, is human beings. Social engineering and phishing scams are becoming increasingly sophisticated as cyber criminals and hackers work to exploit human curiosity.

On 12th May 2017, the NHS was the victim of the largest ransomware attack in history. The WannaCry virus (a form of ransomware) exploits and cripples organisations around the world, affecting 100 countries with over 57,000 infections and each and every infection was the result of somebody simply clicking one wrong link. In fact, end user malpractice can be attributed to a much larger proportion of incidents, compromising security through negligence and/or ignorance.

According to Mimecast, **51% of organisations have suffered a ransomware attack** and on average organisations experienced **3 days downtime** as a result. Time is money, and global cybercrime damages are predicted to cost up to **$6 trillion annually** by the end of 2021.

These figures indicate that migration to the cloud is not itself the greatest risk, but in fact it is careless work practices that undermine security controls. Despite that, only 1 in 5 organisations offer regular awareness training to employees. Employee education through regular training is key to avoiding this sort of catastrophe, however there is something you can do to protect your business. Mobile Device Management (MDM), Multi Factor Authentication (MFA) and a Bring Your Own Device (BYOD) policy can give you enhanced control over end-user behaviour through careful monitoring and security protocols.

Ensuring that in-house security procedures are understood and practised by all your employees is vital to keeping your data safe, regardless of whether a cloud-based solution is used or not.

Conclusion

When migrating to any sort of cloud based IT infrastructure, it's imperative that you know where your data is. If you stay abreast of regulatory changes and work with your cloud provider to ensure that compliance is met at all levels, with a solution that's right for your business's particular requirements, then your cloud security will be as good, if not better that any on-premise solution.

There will always be threats to your data. That's the world we live in. But these risks exist wherever you host your data - in the cloud, or on-premise, and by working with the right cloud provider you can minimise these risks significantly.

Take your time choosing your cloud provider. Ask the right questions and be sure that your provider is reputable, and can offer you a reliable support service. By working closely with the right cloud hosting provider in a true partnership, you can be sure of a solid, flexible and secure cloud solution that you can rely on, which will see your business reap dividends.

Find out more

If you'd like to speak to a Teledata cloud expert about how our cloud solutions might be of benefit to your company, you can **get in touch with our team here**.

We offer a range of services from our Manchester data centres, including active-active cloud hosting; private virtual desktop; private cloud, managed hosting and colocation. Access our full range of services for more information **here**.

teledata™

people and technology together

Teledata UK Ltd

Delta House, Wavell Road, Manchester, M22 5QZ

t: 0161 498 1200 **e:** enquiries@teledata.co.uk **w:** www.teledata.co.uk