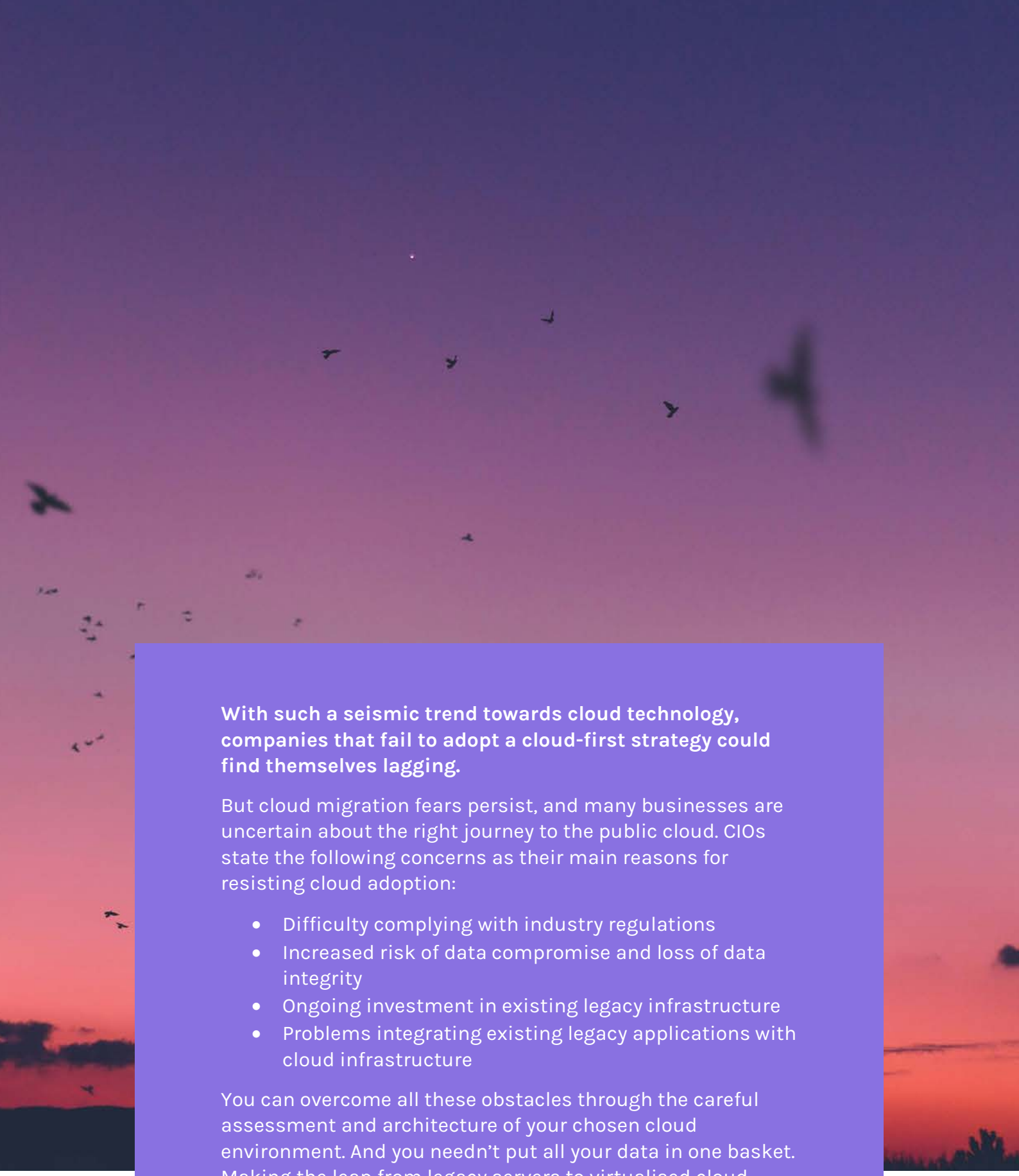
EMBRACING HYBRID CLOUD:

THE REDPIXIE RECIPE FOR SUCCESS

RedPixie

By 2020, a global shift to the cloud will affect £796 billion of IT spending.

GARTNER



With such a seismic trend towards cloud technology, companies that fail to adopt a cloud-first strategy could find themselves lagging.

But cloud migration fears persist, and many businesses are uncertain about the right journey to the public cloud. CIOs state the following concerns as their main reasons for resisting cloud adoption:

- Difficulty complying with industry regulations
- Increased risk of data compromise and loss of data integrity
- Ongoing investment in existing legacy infrastructure
- Problems integrating existing legacy applications with cloud infrastructure

You can overcome all these obstacles through the careful assessment and architecture of your chosen cloud environment. And you needn't put all your data in one basket. Making the leap from legacy servers to virtualised cloud infrastructure is understandably daunting – which is why, at RedPixie, we are strong advocates for a hybrid cloud solution.

HYBRID CLOUD: THE BEST OF BOTH WORLDS

For those unfamiliar with the term 'hybrid cloud', here's a brief summary:

'Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms.'

Of course, the orchestration itself differs depending on your company's specific needs. This guide will outline the best practices for three main areas of hybrid cloud success:

- Assessing cloud environment and infrastructure
- Preparing for hybrid cloud migration
- Managing security and compliance

Adopting a solution that addresses all these aspects will help streamline your company's journey to a cloud-centric workspace.

ASSESSMENT & DISCOVERY: WHAT'S THE BEST ROUTE TO THE CLOUD?

82 percent of businesses are already thriving in a hybrid-cloud environment. But there is no one-size-fits-all strategy for their success. Hybrid cloud migration requires meticulous forethought to architect the right solution for your purposes.

Legacy systems still underpin much of the financial services industry's most critical processes. With 90 percent of IT executives admitting they are held back by outdated applications, a move to the cloud is all but inevitable. So how do you take those initial steps?

Many CIOs are committed to their legacy investments, reluctant to sacrifice expensive hardware for complete cloud immersion. Instead, start by assessing your existing infrastructure and considering which foundational components you can transfer to virtualised servers. The key is to decipher exactly which components of cloud-computing are critical to your business. You can achieve this in four steps:

1. Consider the **administration and business impact** of cloud migration. How will the cloud improve your bottom line? And how many of your processes (core and non-core) are you able to move immediately?
2. Define your **network requirements**. How will you connect your on-premises infrastructure to the cloud? Do your network capabilities support resilience and disaster recovery?
3. Consider **service management** both on-premises and in the cloud. Will you be able to integrate existing management tools with your chosen cloud environment? Or will you need to deploy new, cloud-born management services?
4. Draw up **governance policies and service level agreements** (SLAs). Do your current governance and compliance frameworks resonate in the cloud? Are there identity gaps you need to consider?

While there is no definitive solution to cloud migration, these guidelines are essential to a happy and successful hybrid integration. Once you've discovered the immediate and long-term needs of your business, you can begin to understand where and how cloud computing fits into the bigger picture.

HYBRID CLOUD IN ACTION

We followed this process for a financial client who had exhausted their data centre capacity, enabling them to access the scalability and flexibility of the cloud. They didn't have the CAPEX budget to invest in new data centre storage, so we architected a hybrid solution that connected them with the public cloud. We worked with their cloud provider to implement a harmonious production environment that addressed all the focal points above.

HYBRID CLOUD MIGRATION: THE ROAD TO FUTURE FLEXIBILITY

Although budgetary restrictions are easing, CIOs must still find ways to reduce costs, standardise processes and provide flexible, responsive services. 44 percent of businesses are currently undergoing a digital transformation - a trend that will impact 80 percent of enterprises within the next five years, says Gartner.

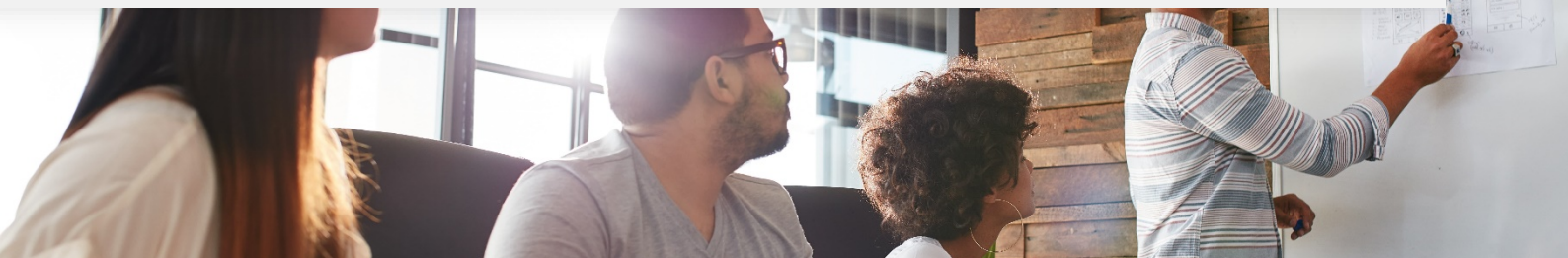
Taking steps towards the cloud is important – even if they are tentative ones. Hybrid cloud is your stepping stone to long-term flexibility and agility, allowing you to spread your workload across both legacy and virtual platforms.

Again, you need to think strategically about the way you approach the actual migration of your data, infrastructure and software. You may decide to keep many of these components in your own data centre, or you might subscribe to an on-demand service such as Microsoft Azure. In either scenario, there are many factors to keep in mind as you begin your journey to the public cloud:

- Security
- Speed
- Flexibility
- Performance
- Cost
- Locality

Which of these are most critical to the success of your cloud solution? If you want to offload sensitive data from vulnerable on-premises servers, then storage and security are likely to be at the forefront of your mind. However, if you are looking to run complex risk modelling calculations in a highly-scalable, mission-critical environment, you may be more concerned with flexibility and performance.

In our experience, a hybrid cloud means you don't have to compromise. You can separate data and workloads between on-premises and public cloud services, securely connecting the two environments to maximise the potential of your business processes. Here's how it's done:



1. CONNECT ON-PREMISES NETWORKS TO THE PUBLIC CLOUD – SETTING UP A VPN OR EXPRESS ROUTE

Companies sending data back and forth between internal and external servers need to ensure the gateway is secure. To do this, think beyond the boundaries of your own firewalls and view them as just one small part of the broader cloud network. Setting up a Virtual Private Network (VPN) will ensure data is protected in-transit between your data centre and the data centre of your cloud provider, even if you automate the process.

To set up a VPN, you need to choose a provider who will keep your network secure over the public internet. While a VPN is technically a WAN (Wide Access Network) it retains the same functionality and security as a private network. Connecting your employees to a VPN is simple:

1. **Perform a data audit**. Work out what kind of data you will be exchanging. This will help you decide on the right VPN protocol.
2. **Set up an appropriate router**. This must have wired and wireless connectivity and built-in VPN functionality. VPNs need good bandwidth to operate effectively.
3. **Consider security options.** It's important to think about user access, encryption and client security when connecting employees to a VPN. Check out the next chapter on security and compliance for more information.
4. **Connect your employees.** VPN deployment is easy. Simply follow the guidelines of your specific provider or use their wizard to connect end-user computers to your network. They will then be able to use a secure login to access the network at home or across public Wi-Fi.

Alternatively, you can set up an Azure ExpressRoute, which allows you to privately connect Microsoft datacentres with on-premises infrastructure, without the use of the public internet. VPNs can be securely linked to the ExpressRoute so that remote workers can access this gateway from anywhere in the world. In both cases, it's vital you secure all servers with strong encryption and firewalls.

2. BUILD OUT YOUR CLOUD ENVIRONMENT

If you're hoping to lift and shift data from your on-premises servers to secure cloud storage, this will mean replacing your existing infrastructure with a VM (virtual machine) equivalent. Virtualised infrastructure allows multiple environments to function on the same physical machine, reducing the cost of data storage and processing.

Equally, you may want to reconfigure an existing application in the cloud to scale it on-demand. As long as you've followed the best practices in the previous chapter, you will have a strong foundation to begin architecting infrastructure and software that meets your requirements.

3. PERFORM A PROOF OF CONCEPT (POC)

With hybrid cloud, you don't have to migrate all your workloads and applications at once. First, you can test non-core processes in your new cloud environment to measure scalability and performance. If these tests produce promising results, you can begin offloading more critical workloads to the cloud as and when increased processing power is needed.

4. MIGRATE USERS

Once you have confirmed the suitability of your cloud infrastructure, you can incrementally migrate users. Moving small groups of users at a time allows you to address any issues that may occur with security or compliance by limiting potential points of failure. If you already have an established user directory such as Microsoft's Active Directory, you can integrate this with your cloud management system.

SECURITY AND COMPLIANCE: EXTENDING YOUR NETWORK INTO THE CLOUD

Hybrid cloud management doesn't end at the migration phase. Businesses need to remain aware of security and compliance issues that aren't present in on-site only systems. But, while 49 percent of IT decision makers have doubts about the network security of public cloud services, these unfounded concerns spring primarily from a fear of change.

Cloud service providers such as Microsoft dedicate a huge proportion of their time and revenue to securing cloud environments – something the average enterprise is unable to achieve. Encryption is an essential part of their security defences, but for those concerned with regulatory compliance, a hybrid cloud can help ease some of their worries and enable them to meet disaster recovery standards.

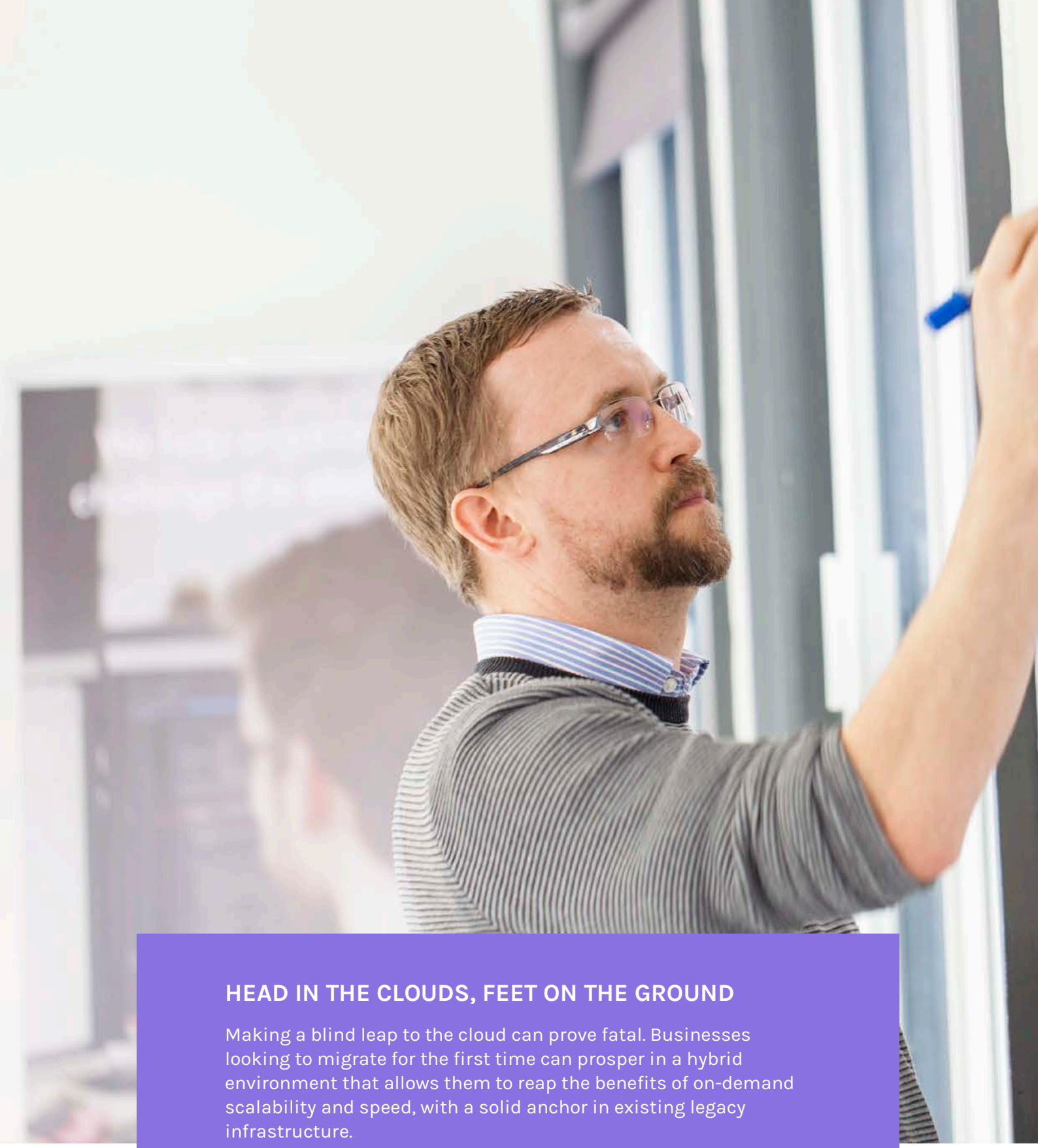
IDENTITY ACCESS MANAGEMENT (IAM)

Securing data in the cloud demands a fresh approach to access management. Since a public cloud is a multi-tenant system, it's difficult to know who's handling sensitive data without some form of identification process. IAM enables IT teams to keep track of user activity and allow privileged access to those who need it via secure authentication processes.

REGULATORY COMPLIANCE

Regulatory compliance requires standardised procedures for data storage, backup and integrity, which is why it's important to choose a cloud service provider that complies with these laws. Local regulations such as the Data Protection Act are just as important as universal directives like the GDPR or SEPA.

In a hybrid environment, companies must implement holistic data governance policies that define a single set of rules for both public cloud and on-premises systems.



HEAD IN THE CLOUDS, FEET ON THE GROUND

Making a blind leap to the cloud can prove fatal. Businesses looking to migrate for the first time can prosper in a hybrid environment that allows them to reap the benefits of on-demand scalability and speed, with a solid anchor in existing legacy infrastructure.

By 2020, a 'no cloud policy' will be as rare as a 'no internet' policy today, says Gartner, as digital transformation continues to revolutionise the financial services industry. To keep pace with your competitors, start the transition to hybrid cloud today. With the help of our cloud architects, you can look beyond technology and into the future of your business operations.

RedPixie

info@redpixie.com redpixie.com/contact-us @redpixie