STaaS MYTHS VS FACTS

Whether your organisation has already taken its first steps towards the cloud or not, it's wise to seek out the facts before making your next move. There are some common misconceptions that surround Storage-as-a-Service (STaaS), and plenty of confusion around the merits of public versus private cloud, particularly when it comes to the costs and risks.

Here, we explode some of the common myths to help you get clarity and steer the right course for your organisation.

Creative ITC

MYTH

Public cloud is cheap compared to private cloud.

FACT

Public cloud resources can become very expensive, very quickly. Often the attractive headline costs are a fraction of the costs you find yourself paying. As well as costs for ancillaries such as IP addresses, failovers, backup and so on, you can end up overpaying or hit with additional charges for:

- Incorrect provisioning and unused instances: If you under-provision, you'll need extra resources at a higher cost, while if you over-provision you pay for resources which are not being used. Right-sizing takes skill and experience.
- Transactional costs: Many public cloud providers charge what a nominal fee for accessing your data, but as your data increases, so do the costs.
- Migration and egress: Moving from one public cloud to another can be costly and difficult. Most providers will bill to extract your data from your current public cloud, so you could find yourself effectively stuck with your cloud provider.
- Data transfer charges: Transfer of data into your public cloud is generally free, but transferring it out is often subject to outbound transfer and bandwidth charges that vary between providers, regions and zones.
- Unhealthy instances, unattached persistent volumes, and unused static IP addresses can all be money sinks too. Then there are attractively priced discount plans on prebooked capacity when you commit over a fixed term. These can offer significant potential savings over on-demand pricing – but only if you use them.

MYTH

Public cloud is easy to manage.

FACT

Your team will need to manage your organisation's use of public cloud if you choose that route – that means customisation, top-level and day-to-day management, optimisation, security, backup and monitoring all taken care of in-house.

This all comes at an additional cost in terms of tools and skilled resource. It's also important to note that anyone within your organisation can sign up to public cloud storage, leading to cloud sprawl, reducing visibility and with it your ability to manage the environment effectively in terms of costs, performance, and security.

As highlighted above in our first myth, mismanagement and a lack of oversight will mean you end up paying more than you budgeted for, so you need people on your team who have the right knowledge, skill and expertise. This means upskilling or hiring new talent and the inevitable additional costs that incurs.

MYTH

Security is the cloud provider's responsibility.

FACT

If you choose public cloud, the onus is on you to ensure your data backup, protection and security are up to scratch, as ultimate responsibility for your data rests with your organisation – not with the public cloud provider. This is the shared responsibility model. It's essential to understand exactly where responsibilities lie when it comes to securing your cloud environment, as it might vary based the services you're using. And although some attackers use highly sophisticated means, it's end user errors that are responsible for the vast majority of data breaches.

MYTH

More security tools mean more secure data.

FACT

This couldn't be further from the truth. More security tools don't equate to better security. A complex cloud environment where you're using multiple disparate security tools from a multitude of vendors, each blocking different attack vectors and not communicating with other solutions is a recipe for high risk. It leaves gaps that are vulnerable to attack.

A safer approach by far is to simplify with carefully selected security tools, or better still to work with a STaaS provider who will implement industry-leading controls and monitoring on your behalf.

MYTH

STaaS means not on my premises and therefore not secure.

FACT

Most MSPs invest heavily in top-end cybersecurity tools, as well as staff who are highly knowledgeable in their field. The ability to defer to your MSP on security reduces the need for you to hire and retain expensive, scarce infosec professionals. MSPs will also be continuously updating their security measures in line with the latest guidance and conducting regular testing.

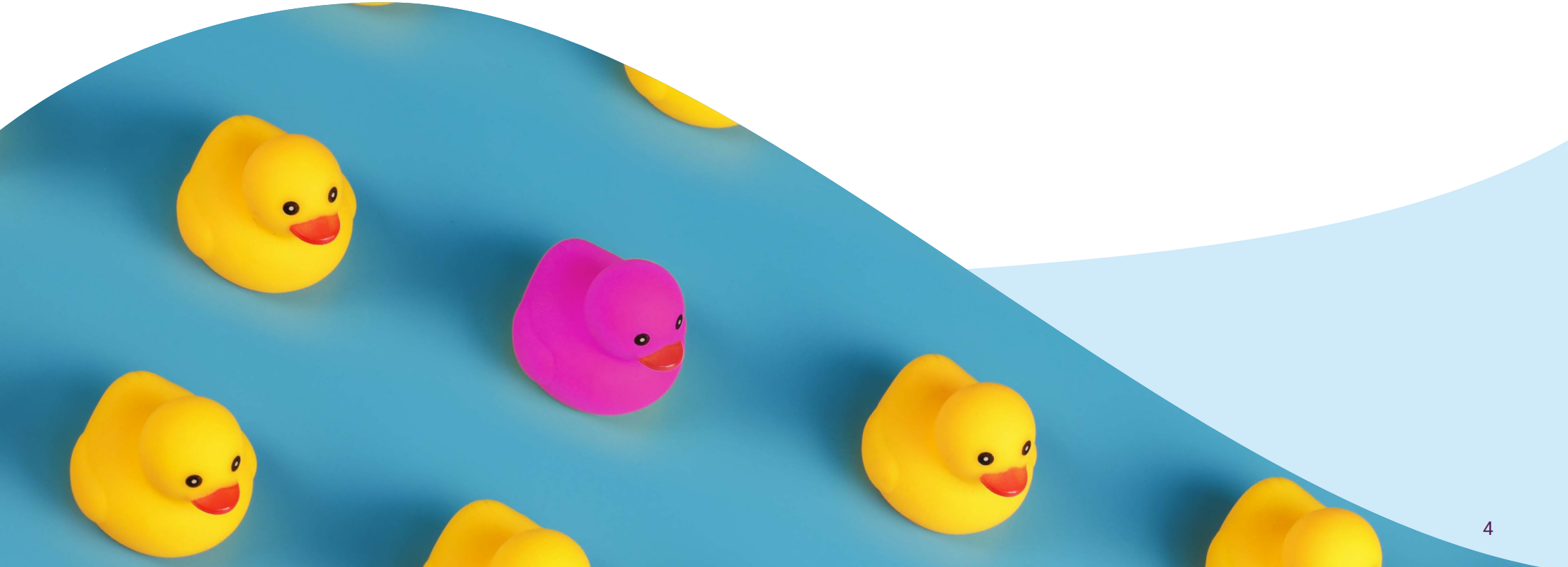
STaaS can be tailored to suit your specific needs, not only in terms of capacity and performance but in terms of security too. One security advantage of hybrid cloud infrastructure is the flexibility to decide where applications and data will reside, in a private cloud or datacentre. If you need certain data to stay on-premises, some STaaS offerings, such as Creative ITC's, can also accommodate this.

MYTH

STaaS is a purely cloud-based service model.

FACT

While cloud is an important part of STaaS, some MSPs (Creative ITC included) also offer the option to store data on their own premises, as mentioned above. This is effectively an on-premise deployment, but you would still only pay for what you use – rather than investing in expensive hardware that may never be fully utilised and will have a limited lifespan. This is an ideal solution for those organisations that are not yet ready to put their data in the public cloud, but who don't want to keep investing in high-spec servers and paying dedicated storage teams.



If you have any questions about these myths or other storage queries, email **hello@creative-itc.com**

To discuss STaaS for your organisation, call **+44 (0)20 4551 9267**

Creative ITC