CLOUD SECURITY

A SHARED RESPONSIBILITY

WHITE PAPER

advance

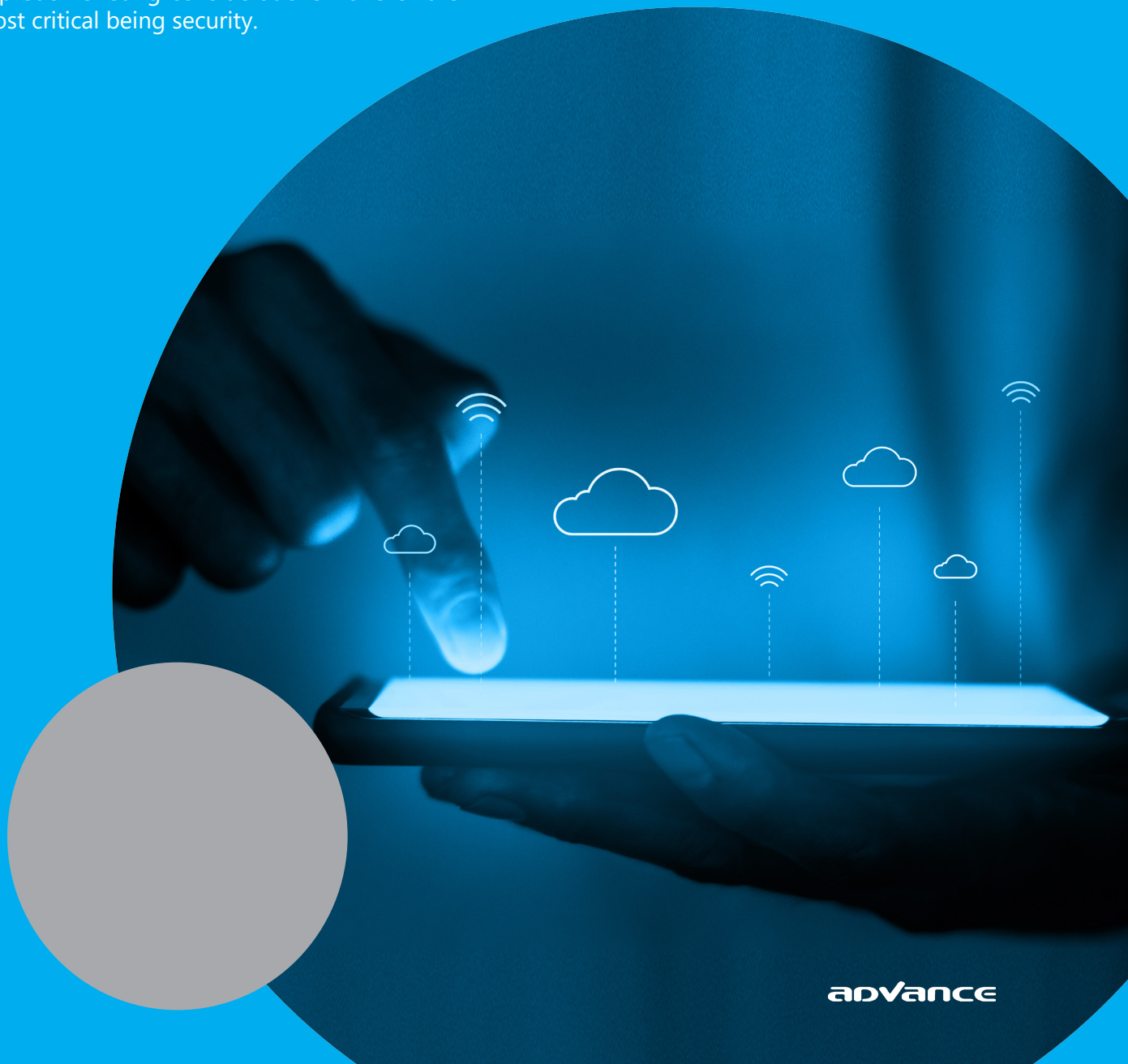
INTRODUCTION

Ten years ago, 'cloud' was considered a buzzword. Now, for many of us, the cloud has joined our everyday vocabulary at work and at home. We use the cloud to improve and enhance the experience of many tasks and services. From photos with invisible cloud backups, to email, which runs almost exclusively on the cloud today.

The appeal of cloud-based business services is simple: they offer scalable, flexible, cost-effective solutions that allow any organisation, particularly small and medium enterprises (SMEs), to become more efficient and more competitive. However, as with any technological innovation, cloud computing also introduces a new realm of considerations and new ways to approach existing considerations—one of the most critical being security.

While it would be nice to say that security in the cloud is purely the responsibility of the cloud service provider, the reality is that such an important responsibility must be shared between the cloud provider and the consumer. However, 'cloud' is a broad term that describes several different technical frameworks, and the security responsibilities are shared differently in each.

This paper will cover the three most common cloud frameworks and how security responsibilities are split between the provider and consumer.



UNDERSTANDING CLOUD SECURITY

The term 'in the cloud' simply refers to a service provided by hardware in a data centre managed by another party. It might be a private cloud offered by a local provider; a public cloud provided by Microsoft, Google or Amazon; or a software service like Salesforce or Xero. There are three main types of services that can be delivered in the cloud: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

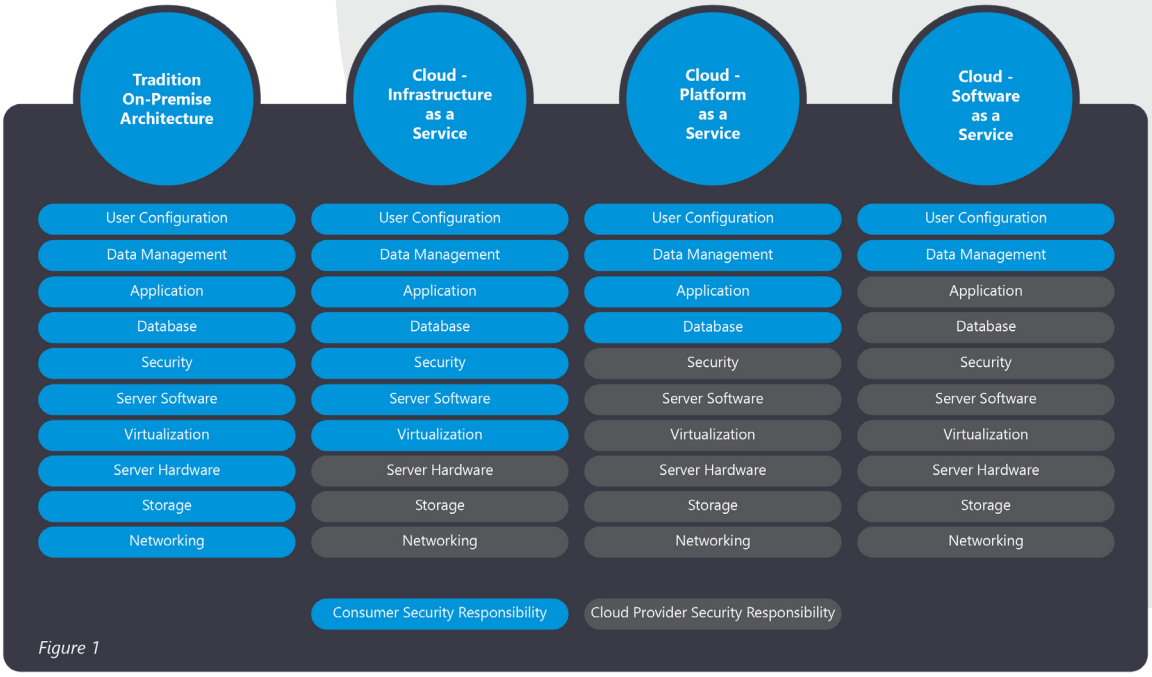


Figure 1

In **infrastructure as a service**, the cloud provider supplies access to hardware and a virtualisation layer, allowing the consumer to run a traditional IT ecosystem without the upfront investment in hardware. In this setup, the cloud provider takes on responsibility for the physical security of the hardware, as well as some basics around the network and virtualisation layer. All other security activities remain with the consumer, as shown in Figure 1. This means the consuming business must still patch their servers, configure the networking, firewalls and applications securely, and more.

Platform as a service is the next level on the cloud computing spectrum. Under this arrangement, the cloud provider supplies access to a platform—most commonly a database layer—on which the consumer can build applications. This set-up moves more security responsibility to the cloud provider, but much still resides with the consumer.

Finally comes the most common solution in the SME space, **software as a service**. Most websites that require a subscription fee are Software as a Service cloud implementations; common examples include HubSpot, Canva and Xero. In this set-up most, but not all, responsibility for security resides with the cloud provider. Consumers of SaaS apps are unlikely to need to worry about patching and security updates; however, importantly, some security considerations still reside with the consumer. The consuming business still has control over many user and account attributes that contribute to security, as well as what data enters the SaaS product and with whom it's shared.

There are no cloud implementations where the consuming business has no role in keeping its data secure.

Even for the security elements under the cloud provider's control, consumers should understand their practices and ensure they're appropriate for their particular type of data.

For example, when evaluating a new online accounting software package, a business may identify that the data that will be added to the software is sensitive in nature. As a result, they may want the data encrypted. While the business doesn't have control over the encryption of data, it's still responsible for selecting a cloud provider that encrypts data, as well as ensuring the advertised encryption takes place.

Perhaps the best analogy for shared security responsibility in the cloud is a gated community. Management may provide security for the community in the form of a front gate, but it's up to each resident to lock their own doors.

KEY CONSIDERATIONS FOR IMPLEMENTING CLOUD SECURITY

Implementing cloud security for a business requires careful consideration and planning, and it's not a task that should be taken lightly or rushed. Here are some important things to consider:

RISKS AND BENEFITS

The risks and benefits of cloud security are almost identical to those of on-premise security. Cybercriminals aren't concerned with whether data resides on-premise or in the cloud, and similarly, the business consequences of a cyber incident are generally the same for cloud data as for on-premise data.

UNIQUE SECURITY NEEDS

Every business is unique, and so are its security needs. Some industries handle more sensitive data than others, and thus may require stronger security measures. Identifying the type of data that will reside in the cloud, understanding the regulations around this data, and assessing the risks to tailor a cloud security strategy are all critical factors.

SELECTING A RELIABLE CLOUD SERVICE PROVIDER

Cost isn't the only factor in choosing a cloud provider; be sure to also consider their commitment to security. After all, the provider will often be the first line of defence when vulnerabilities or threats arise. Make sure they adhere to industry security standards, provide transparency in their security policy, and offer robust security measures such as data encryption, firewalls, intrusion detection, and regular security audits.

REGULAR REVIEW AND UPDATING OF SECURITY MEASURES

Cloud security isn't a 'set and forget' endeavour. It requires regular reviews and updates to ensure that the measures in place are still effective and updated with evolving threats. Consider implementing a periodic security review process in business operations.

PARTNERING WITH A TRUSTED CYBERSECURITY COMPANY

While every business should understand the basics of cloud security, SMEs without a dedicated IT department might need help navigating the complexities of implementing and maintaining robust cloud security. That's where partnering with a trusted cybersecurity company can be incredibly valuable.

Cybersecurity organisations specialise in protecting digital environments, and their expertise can help ensure that cloud security measures are comprehensive, up-to-date, and aligned with business needs. Here's how a cybersecurity partner can contribute to cloud security:

EXPERT GUIDANCE

A knowledgeable cybersecurity partner can help a business understand its unique security needs and advise on the most suitable security measures. They can help navigate complex regulations and industry standards, ensuring a cloud environment or service is compliant.

ONGOING MONITORING AND MANAGEMENT

Cybersecurity companies offer services to monitor cloud environments continuously, quickly identifying and addressing potential threats or breaches. They can manage the regular updating and patching of the cloud systems that require it, relieving this burden from the consuming organisation.

RESPONSE PLANNING

In the event of a security incident, a quick and effective response is crucial. A cybersecurity partner can help develop an incident response plan, ensuring a business is prepared to handle potential breaches.
Remember, implementing and maintaining robust cloud security measures isn't just a task to tick off the list quickly and move on—it's an investment in a business's future. By protecting data, an organisation is safeguarding its reputation, its financial stability, and the trust of its customers.

CONCLUSION

SAFEGUARDING YOUR BUSINESS WITH CLOUD SECURITY

In the digital age, the need for dependable cloud security cannot be overstated. As our reliance on cloud computing continues to grow, so does the necessity to protect the data and applications that live in this environment.

Each of the three types of cloud arrangements—IaaS, PaaS, and SaaS—comes with a different balance of security responsibility between the provider and the consumer; however, in every case, the ultimate responsibility rests with the consuming business.

Modern SaaS applications often make it seem like all of the security is being handled by someone else, but this is rarely the case—and it's an especially dangerous mindset for business owners, who need to be vigilant to not only do their bit but also ensure their cloud provider takes security seriously.

Again, cloud security is like a gated community. Somebody is responsible for the security of the outer gate, somebody else is responsible for locking the front door—and somebody is responsible for everything in between. The key is understanding who's responsible for what, and ensuring it's being done.

used in their organisations, communicate this to their users, and implement policies and technical controls to manage this usage actively.

advance

Contact Info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au