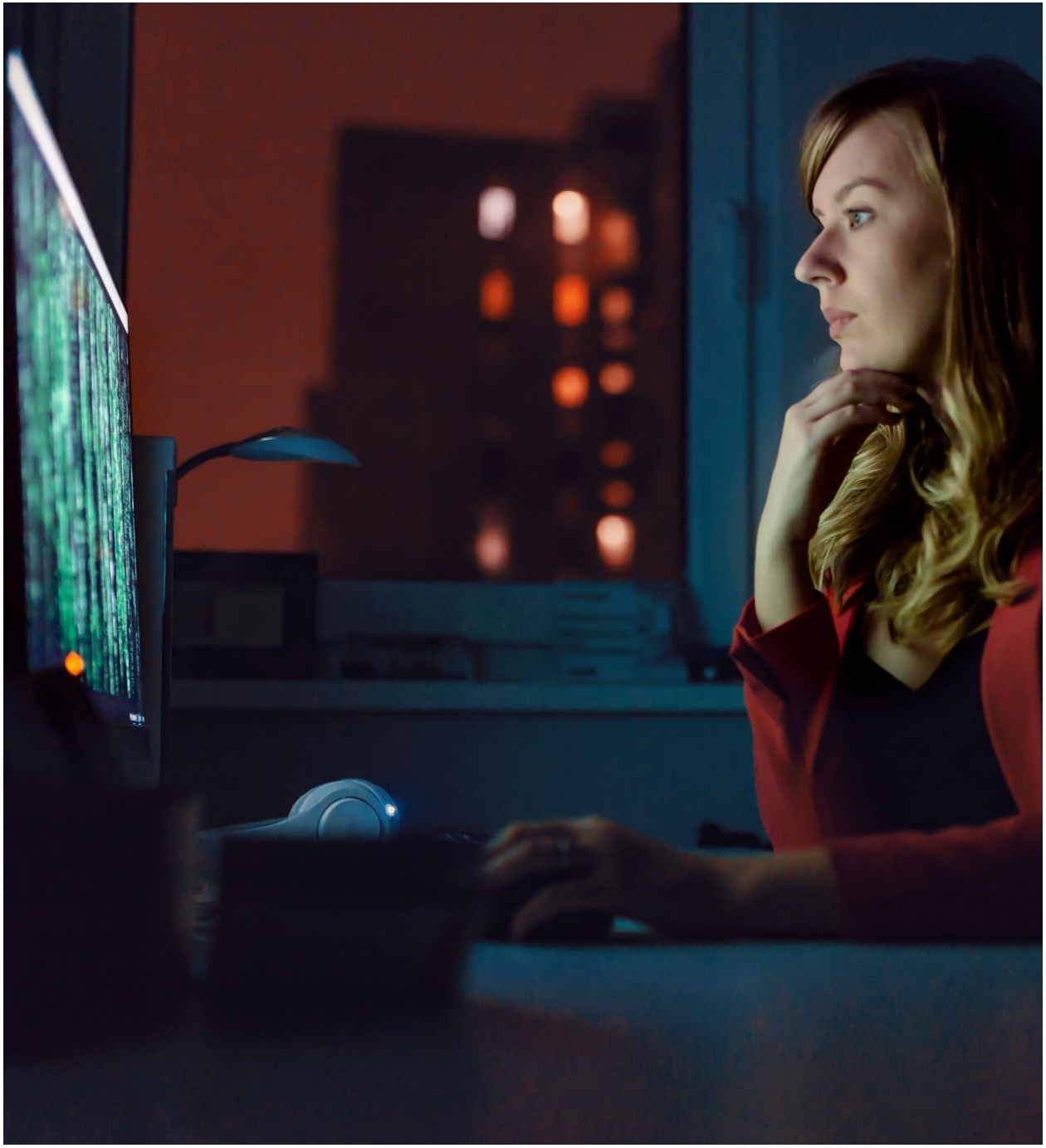

BT
Cut your
security risks
by choosing cloud

# Contents





# Introduction

It's difficult to remember a time when there wasn't a constant wave of security threats. Just as the dust begins to settle on the Microsoft Exchange exploits, we'll be faced with the next high-profile incident.

Yet again, some of the software and systems behind our organisations' operations will be under threat. It might be an old vulnerability with a patch that's been available for a while with low take up, but now an exploit has emerged.

It might be something brand new with a patch fresh out from the vendor. Worst of all, it could be a zero-day vulnerability with no current fix. In organisations around the world, incident teams will be asking, "is this an issue for us?"

We think organisations can help to break this pattern – or at least reduce some of their risk burden – by accelerating their move to the cloud.

Using public cloud services puts some of the responsibility for the underlying infrastructure onto the providers, all of whom are highly motivated to keep on top of the situation. A public cloud environment also attracts a greater degree of scrutiny from vulnerability-hunters than a private one, helping in the fight to stay protected.

The way you run patching in the cloud can also make security easier. Some aspects can shift to the provider altogether and others can take place without impacting your service availability.

Not all the risks and responsibilities shift to the cloud provider, however. Organisations still need to bring in external tools and services to assess and report on the security of their cloud services, while continuing to keep a clear overview of where and how their data and assets are stored.

**In this paper we'll explore the ways in which you can reduce your security risk by using the cloud, as well as additional aspects of cloud security you'll need to consider. We'll finish with recommendations for how to implement security for a cloud-first model in stages; immediate actions, mid-term moves and ambitions for the future.**


# Vulnerabilities are a fact of security life

Security vulnerabilities will keep on coming, no matter how advanced our technology.

Humans are imperfect, and the code they create will always come with a risk of flaws that could compromise confidentiality, integrity or availability – cloud services aren't immune from this.

Historically, software vulnerabilities have mainly been identified by skilled attackers, only coming to light post-compromise. More recently, the security industry has shifted to relying on the work of ethical hackers, with significant success.

However, as an industry, we've applied a disproportionate amount of effort to achieving an incredibly difficult aim – identifying 'unknown unknowns'. But are we doing this at the expense of more obvious defences? And is cloud migration an opportunity to do things differently – even better?

# Patching is a complex issue

Every sound piece of security advice has a section early on that emphasises the critical importance of keeping software up to date to avoid any known vulnerabilities.

However, it's a lot easier to give this advice than it is to make it a reality – and it appears that many organisations are struggling to implement it.

If we look at the statistics on the root cause of major incidents that used vulnerabilities to succeed, it's common to see exploits of vulnerabilities that are more than 12 months old. Research from Ponemon/IBM reported that, "in respondents whose organisations had a data breach in the last two years, 42% said they occurred because a patch was available but not applied"[1].

Even though they are aware of the importance of patching, many organisations are ignoring specific, non-critical risks and are choosing to keep their software several releases behind the latest version.

Some are worried patching will cause some software to break, some struggle to find the capacity to test every single patch for compatibility, and others are overwhelmed by the sheer number of patches from vendors. Moving to the cloud is an opportunity to change this pattern.

## Cloud can significantly simplify patching

When you work in the cloud you can shift the accountability for patching some aspects of your infrastructure to your service providers. Often, they use software-defined mechanisms for patching which don't interrupt your services and you may not even notice updates happening.

Equally, where you're using cloud to run software you're accountable for, there are ways to keep critical services up to date more easily. You can use the elasticity of cloud to take individual components out of service without impacting availability - if they're designed correctly.

# But patching alone is not enough to protect against attack

Most vulnerabilities expose an individual system or capability, but that's usually just the first step in an attack.

Once a piece of malware or a crafted attack has gained initial access, the attacker usually looks to execute code that allows them to get to something else, like exploring the network or stealing data from the affected system.

Once identified, this initial point of entry and whatever the attacker goes on to do (such as pivoting to another system or encrypting your data for ransom) will determine the priorities for the defensive team looking to actively respond.

In all likelihood, the defensive team will close the initial access method, either by patching, password reset or even a system restart.

However, it's common for the attackers to set up alternative access methods (additional backdoors).

This is in preparation for the next stage in the intrusion, as defined by MITRE in the ATT&CK framework - to achieve persistence or maintain their foothold.

In the recently disclosed 2021 Microsoft Exchange Server vulnerability, some victims have reported multiple backdoors in their systems, with one organisation identifying eight separate backdoors.

# Remediation is critical

When an organisation is dealing with 'a hole in the fence' such as the 2021 Microsoft Exchange Server vulnerabilities, of course patching is important.  But that's not the only thing to do, or even the most important element. Understanding whether you have been compromised in any way is critical.

### You should ask yourself:

- what data may have been exfiltrated?
- what might an attacker have learned from that vantage point that would help them elsewhere?
- is there any indication that the attacker tried to establish persistence on the affected assets or moved laterally from them to another system?

Only when you can reliably answer those questions, and have dealt with any further implications can you close the incident - and stand by for the next one.

# Cloud can reduce your security risk burden

In general, the large common cloud systems that many organisations rely on are safer than personal or organisation-specific cloud systems. That's quite a sweeping statement, but let's unpack it a little further.

Large cloud systems are no more immune to vulnerabilities and problems than any other system. But being big and commonly used brings two clear positives: first, that such systems are public and accessible to all, and second, that the incentive to fix them is very high.

## Accessibility means more people can look for vulnerabilities

When a cloud system is accessible to all, the security research community can get to it easily, something that's not possible with a system in a private environment.

They work diligently to identify and responsibly disclose vulnerabilities before they can be weaponised by adversaries. In fact, 2020 saw a record number of vulnerabilities disclosed, with over 18,000 recorded[2]. There's a thriving ecosystem of such teams, spurred on by professional motivation and bug bounty programmes from vendors.

One of the key strengths for the cloud provider's defending team is the responsible disclosure process, where researchers give the vendor advance notice of their findings (typically three months). This gives the vendor time to investigate the issue and issue a fix. Then the researcher can go public with their work.

By way of example, back in October 2020, a security research firm published details of a vulnerability in Azure, specifically the Azure App Services. In this case, the flaws were fixed before they went public.

## The incentive for cloud providers to fix is high

With so many of their customers reliant on shared common systems, the pressure on vendors to fix their systems - either proactively before an attack, or very quickly after attack - is immense.

History shows us that the high-profile nature of such incidents combined with the large development and support teams of vendors lead to quick fixes.

Large players like Microsoft will always have more people and resources to patch systems than a typical enterprise.

Plus, the shared nature of cloud infrastructure and the service elasticity it brings means providers can upgrade individual elements without too much impact on availability.

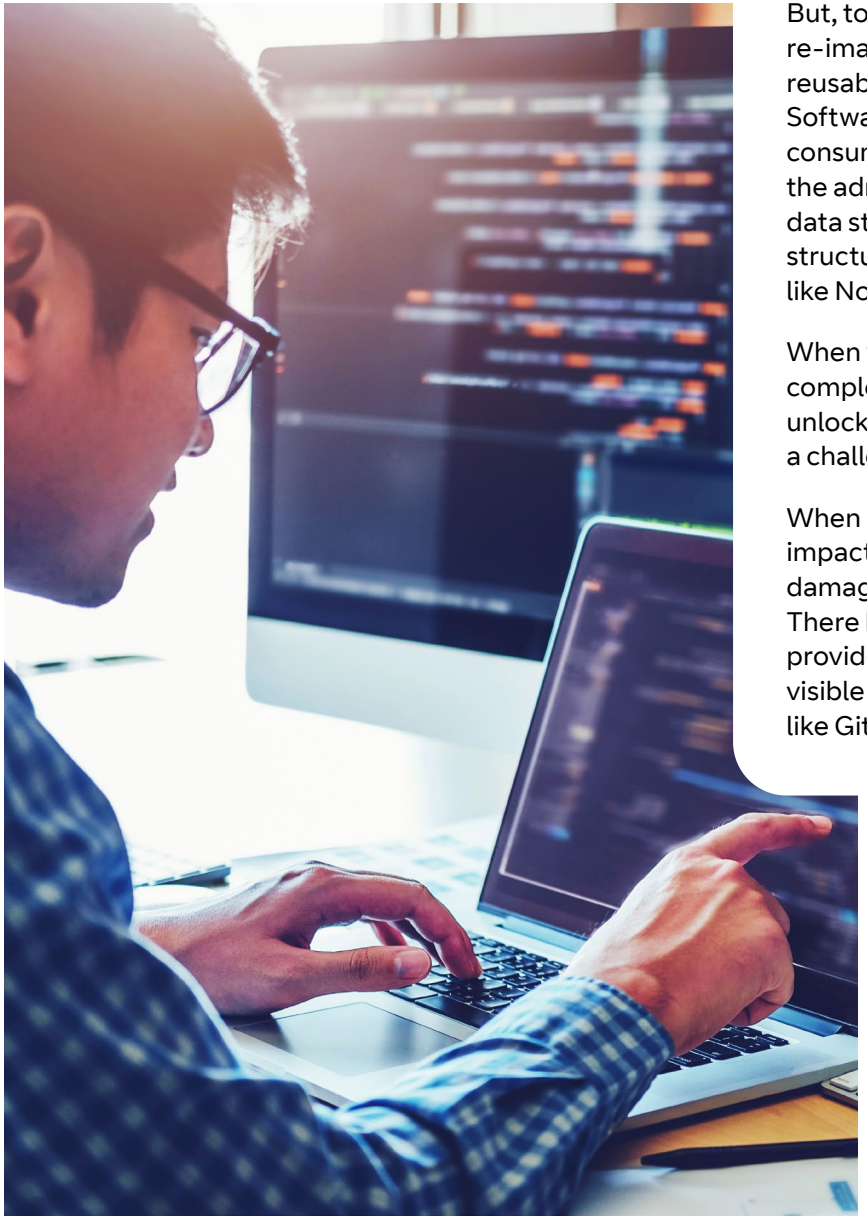
If we compare this patching approach with the track record of the average organisation, the average organisation doesn't come out well. A number of the most high-profile events of recent years, WannaCry and NotPetya included, were avoidable - if your organisation was on top of patching.

# Securing a cloud-based world

While the cloud provides a number of clear security advantages, there are still downsides we must be aware of. Yes, its agility and flexibility around the creation of cloud solutions is incredible. Plus, it offers an enormous scope of services and facilities, and it's so easy to rapidly 'spin up' capability in the cloud.

However, this power and choice comes with immense amounts of complexity that's not always easily visible. Plus, the underlying functionality in hyperscale cloud (like key management and routing) can be very different from the traditional world. It's easy to make mistakes in this environment.

Many companies simply replicate their internal on-premise infrastructure in the cloud.



But, to gain real advantage, organisations need to re-imagine their solutions, building them out of reusable Platform as a Service (PaaS) components or Software as a Service (SaaS) modules. For example, consuming a database as a service can cut out many of the administrative overheads of running fault-tolerant data stores. And if your application doesn't need structured databases anymore, then newer 'services' like NoSQL can be more efficient and effective.

When you can create corporate infrastructure in minutes, completely changing your architectural approach and unlocking a huge scope of service, security can be a challenge.

When a cloud service is largely public by design, the impact of even a small security issue can be extremely damaging, both financially and in terms of your brand. There have been countless incidents on major cloud provider platforms where data has been left publicly visible or keys have been left exposed in code repositories like GitHub.

***"Building and leading a cloud security program is not just about the technical controls; it's about the management, governance, people and process items as well. It's not just about implementing the right technology; it's also about the overall mission and vision of the organization.[3]"***

# Who does what when there's a security incident?

When major incidents occur, it raises a lot of questions about the role of the service provider in the event.

It could be argued that services you consume as SaaS or PaaS involve some level of accountability from the service provider when things go wrong; after all, they're accountable for producing and operating their services.

For Infrastructure as a Service (IaaS), the accountability shifts much more towards the client as they're effectively using cloud hardware to build their solution. In this case, assuming the underlying tool or material wasn't to blame, most incidents track back to the way the solution was built or architected by the client.

There are some grey areas, though, and with some cloud solutions combining IaaS, PaaS, and SaaS to form a final solution, who exactly is accountable and responsible for security can be much less obvious.

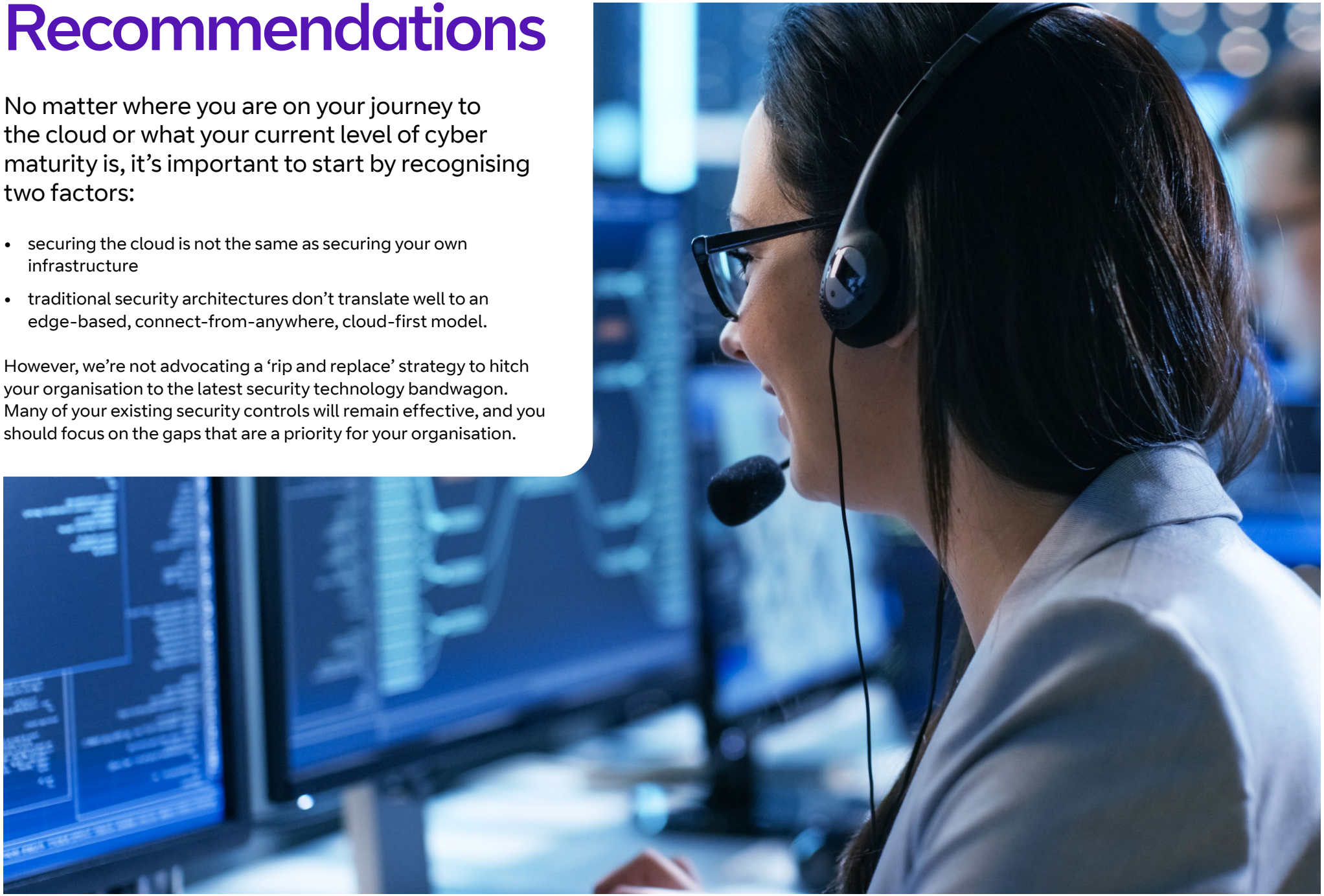
Even though most cloud providers are increasing the tools and reporting that they provide to assure the security of solutions, many organisations still need to bring in external tools and services to assess and report on the security of their cloud services. We're seeing a significant growth in requests for help to improve or report on organisations' security in the cloud. We're also actively building out our offerings around Secure Access Service Edge (SASE) and cloud security services to help organisations with this move.

# Recommendations

No matter where you are on your journey to the cloud or what your current level of cyber maturity is, it's important to start by recognising two factors:

- securing the cloud is not the same as securing your own infrastructure
- traditional security architectures don't translate well to an edge-based, connect-from-anywhere, cloud-first model.

However, we're not advocating a 'rip and replace' strategy to hitch your organisation to the latest security technology bandwagon. Many of your existing security controls will remain effective, and you should focus on the gaps that are a priority for your organisation.



# With that in mind, here are some recommendations for next steps:

## For action immediately - understand where you are and fix what you can

We always recommend that organisations focus on the basics of asset and inventory management, vulnerability and configuration management. Make sure your patch process is as robust as possible.

But beyond that, look to assess your current security posture against the MITRE ATT&CK framework and combine it with threat intelligence to identify the tactics and techniques that pose a risk to you. From here you can prioritise any gaps that you uncover.

For those organisations who have sizeable Operational Technology estates, we recommend undertaking the same assessment using MITRE ATT&CK for ICS.

Work on building up your capability to quickly identify whether your organisation is at risk from the latest discovered vulnerability, and implement new or compensating controls. An ideal first step is to baseline your current coverage using a threat prioritisation framework and identify the next steps to take to close any loopholes.

## In the medium term - migrate to cloud and strengthen detection

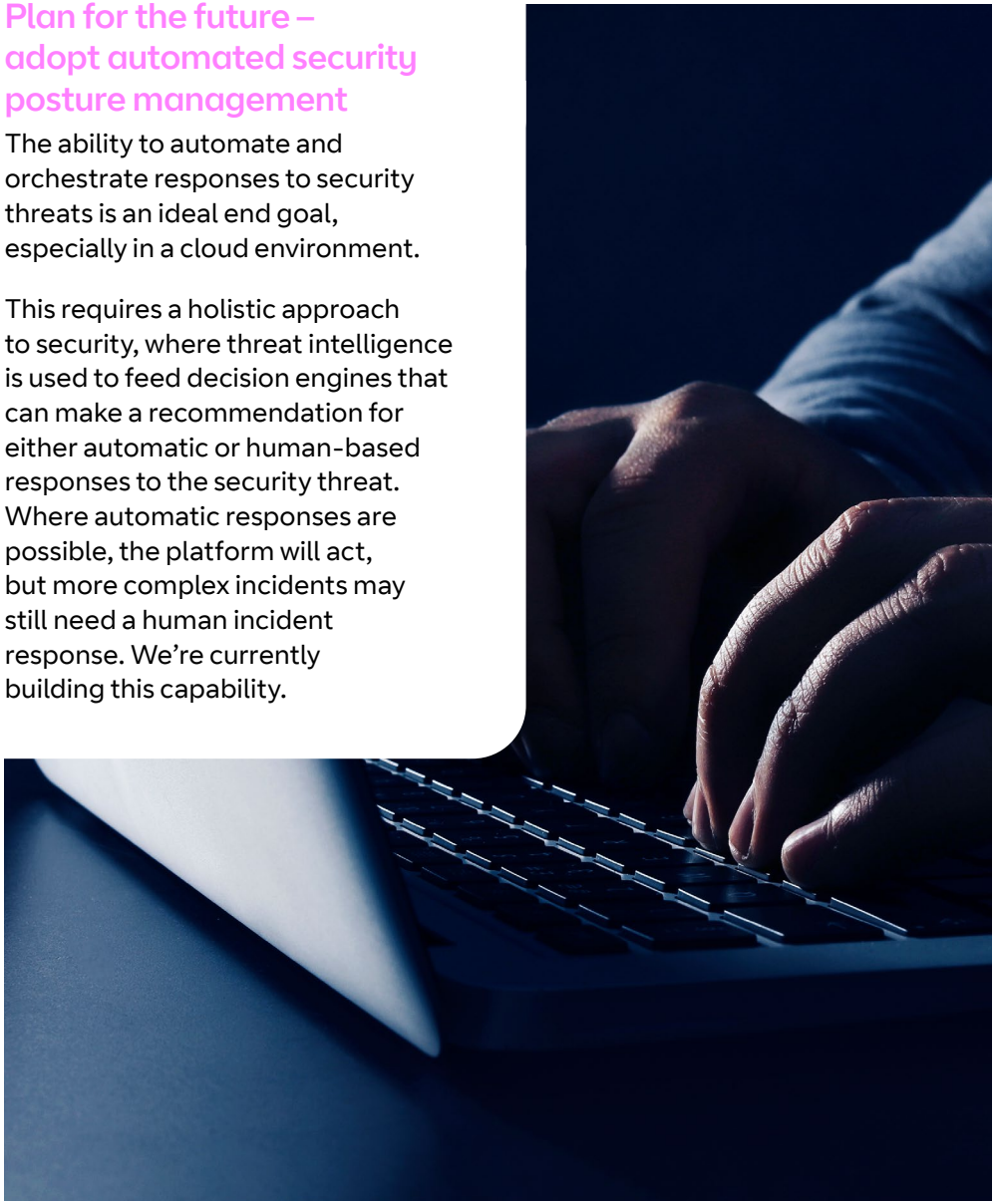
As more workloads move to the cloud, understanding your increased risk is important. Our cloud security roadmap and cloud security maturity assessments can help identify areas to focus on. Also look at how your organisation is positioned to move towards a Zero Trust approach.

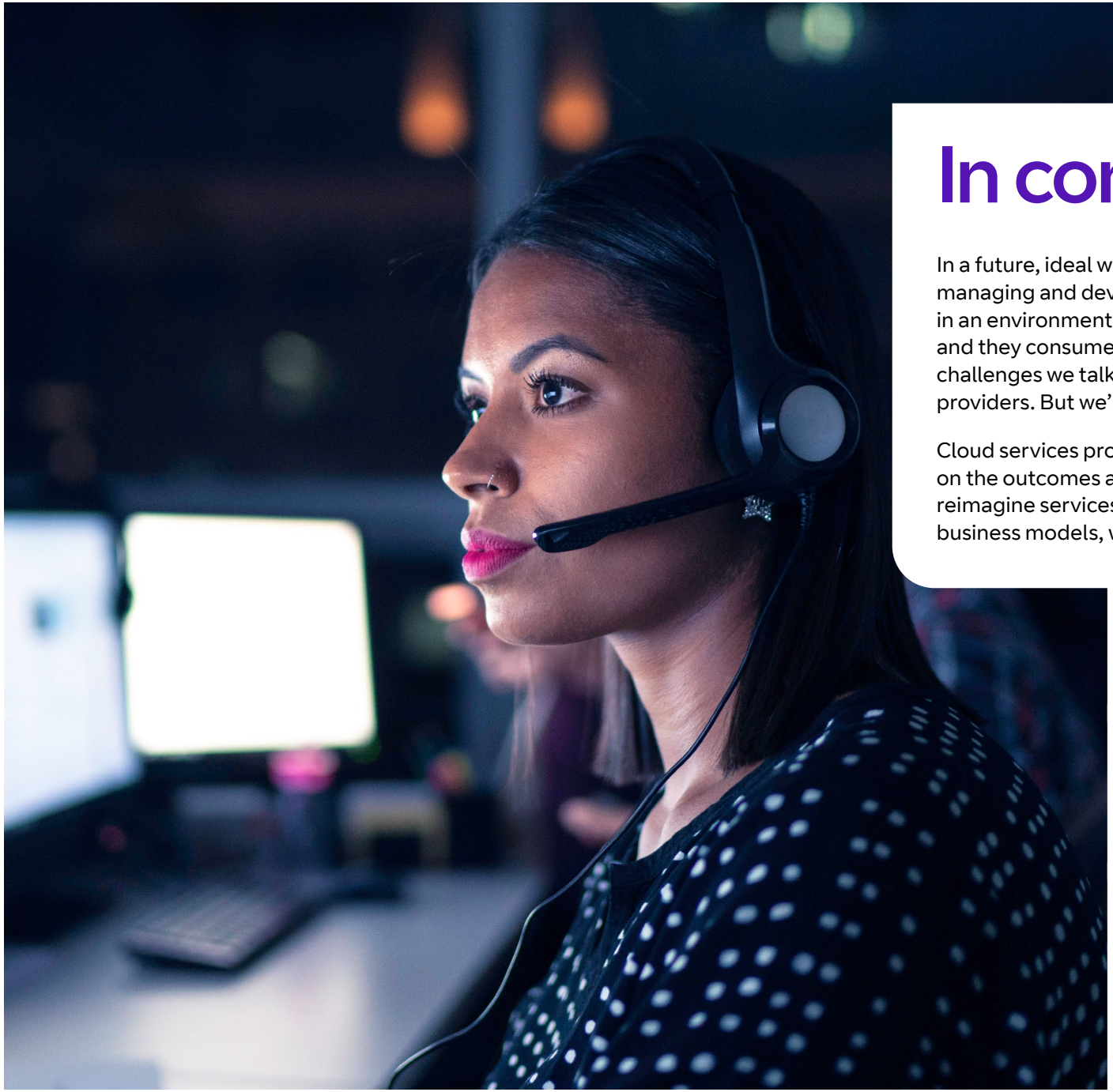
It's also worth considering how to improve your threat detection capabilities. Cloud native controls offer a rich view of activity and there are a host of overlay controls that can help you to see further. However, deploying more controls that generate more data and more alerts is often not the answer, because it creates overwhelming noise for your security team. It can help to add specific targeted threat intelligence to help prioritise and tune your use cases, as can outsourcing some level of your security operations to a managed security services provider.

## Plan for the future – adopt automated security posture management

The ability to automate and orchestrate responses to security threats is an ideal end goal, especially in a cloud environment.

This requires a holistic approach to security, where threat intelligence is used to feed decision engines that can make a recommendation for either automatic or human-based responses to the security threat. Where automatic responses are possible, the platform will act, but more complex incidents may still need a human incident response. We're currently building this capability.





# In conclusion

In a future, ideal world, organisations won't have the burden of managing and developing infrastructure. Instead, they'll operate in an environment where their core services are delivered via SaaS and they consume network infrastructure as a utility. Many of the challenges we talk about in this paper will have shifted to service providers. But we're not there yet.

Cloud services provide an incredible opportunity to focus more on the outcomes and less on the technology. Organisations that reimagine services for the cloud, rather than replicating current business models, will achieve the greatest gains.

As you build cloud-based services, it's critical to bake 'security by design' and 'privacy by design' into your transformation programmes and to factor data management (and protection) in early.

'Assume breach' remains the default security state for many, and this should continue as you move to the cloud. But it's important to remain open to new security opportunities that may emerge as you migrate.

Demand for cloud skills often outstrips supply, so plan to partner or ask for support to achieve your cloud transformation. Partnering is a robust way of accessing detailed, current knowledge about hyperscale services as well as cross-industry experience to avoid mistakes others have made.

# Why choose us to help you with cloud security?

**With our extensive experience helping businesses move to the cloud, you can:**

- avoid common pitfalls and ensure your services are configured correctly to protect against the most up-to-date threats
- get strategic cloud security advice and solutions from our expert advisory teams to match your evolving needs
- evaluate the security of individual services and identify where you may need augmented controls so that even complex and sensitive processes are protected
- see clearly how everything knits together including on-premise, SaaS or IaaS services
- enforce clear policy controls to mitigate the effects of a shadow IT estate
- embrace the fast, flexible, and agile benefits of cloud consumption without increasing security risk.

## Our security services

We're helping customers thrive by delivering world-class security solutions. We have operations in more than 180 countries and support some of the world's largest companies, nation states, and critical national infrastructures. That gives us a unique perspective on cybercrime. Our team of 3,000 security experts and 16 global security operations centres are here to help you keep watch and act decisively at all times.

# References


[1]Ponemon/IBM X-Force Red:
"The state of vulnerability management in the cloud and on-premises", August 2020

[2] Cyber Reports: "Highest Number of Vulnerabilities Disclosure Reported in 2020", February 2021

[3] AWS Marketplace: SANS practical guide to security in the AWS Cloud

## Offices worldwide