

CLOUD.TRANSFORMED.

MANAGING COMPLEXITY IN THE ERA OF THE CLOUD

As cloud adoption continues to grow, so too will the gaps in cloud security. How can you secure your cloud across hybrid, multicloud environments? Read this white paper to find out more.

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	3
2	THERE'S NO BUSINESS STRATEGY WITHOUT A CLOUD STRATEGY	4
3	THE DOUBLE-EDGE SWORD OF THE CLOUD	5
4	WHAT KEEPS THE CISO UP AT NIGHT: THE MULTICLOUD SECURITY CHALLENGE	7
5	HOW TO REDUCE RISK IN A MULTICLOUD ENVIRONMENT	8
6	THE FIVE PRINCIPLES OF CLOUD SECURITY	9
7	TOP CLOUD SECURITY FEATURES AND FUNCTIONALITIES	10
8	ITC'S APPROACH TO CYBER SECURITY	11
9	USE CASE: INTERNATIONAL TECHNOLOGY COMPANY IMPROVES ITS CLOUD SECURITY POSTURE WITH ITC	12
10	FINAL THOUGHTS	13

Section one

EXECUTIVE SUMMARY

Most organisations today rely on at least one public cloud and those looking for better flexibility, agility, ROI, and the ability to diversify risks are embracing the hybrid or multicloud. As cloud adoption continues to grow, so will the gaps in cloud security.

92%

of organisations
admit to a gap in
their cloud security.¹

79%

of organisations have
experienced a cloud-
based data breach.¹

\$3.61m USD

is the average cost of a
breach in a hybrid multicloud
environment.³

Over the past few years, many high-profile breaches have served as reminders that the consequences for businesses with weak cloud security can be significant. Yet many of these same incidents could have been prevented if there was a better understanding of the considerations required for effective cloud security.

With so many cloud security tools, solutions, and services out there, how do you know what the right approach is for your business? This is a key question because technology alone will not solve your security problems.

This paper is designed to help you find out how to effectively address the risks in your cloud environment, together with key considerations to bear in mind, especially as a multicloud strategy gains popularity resulting in more complexity to navigate.

What are the gaps in cloud security?

»» SKILLS

Current cyber skills gap is more than 2.72 million professionals globally.

- (ISC)²

»» TECHNOLOGY

Companies average 43 separate IT security and security management tools in its infrastructure.

- The Foundry

»» GOVERNANCE

Companies take an average of 275 days to identify and contain a data breach.

- Ponemon

Section two

THERE'S NO BUSINESS STRATEGY WITHOUT A CLOUD STRATEGY

Cloud computing is no longer just a buzzword that CIOs or technology enthusiasts talk about for innovation projects. It has become more than just a technology conversation.

Cloud strategy is now a topic that belongs on the executive management and board's agenda. It is at the foundation of the new way of operating. It is the default way in which enterprises interact with customers, suppliers, and stakeholders today.

Businesses have embraced cloud computing for migrating workloads, adopting SaaS applications, implementing DevOps initiatives, and facilitating hybrid work. Governments and public sector too have slowly discovered the benefits of cloud services from streamlining operations, managing costs, ability to scale, and even security.

Underneath all that, it is the consumer who is driving the demand for cloud. The consumer is the one who relies on cloud for every digital service consumed today: from emails to images to social media and streaming music or movies to connected cars and autonomous internet of things (IoT) infrastructure.

“Over 85% of organisations will embrace the cloud-first principle by 2025.”

- Gartner

It's no surprise that that, according to Gartner, “over 85% of organisations will embrace the cloud-first principle by 2025, with over 95% of new workloads being deployed on cloud-native platforms (up from 30% in 2021)”.

Section three

THE DOUBLE-EDGE SWORD OF THE CLOUD

Recognising that there is no business strategy without a cloud strategy, IT leaders are working to create cohesive cloud strategies that are both expansive and forward looking in order to reap the full business value of the cloud – not only to drive technological innovation, but also to serve as the foundation for business innovation.

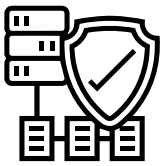
Whilst the benefits of adopting a cloud-first principle are clear, the challenges when it comes to securing your cloud should not be underestimated, especially as more businesses are increasingly turning to a multicloud strategy, which further adds to the complexity of the environment.

The consequence of ignoring cloud security can cause large-scale impact. Just recently, Pegasus Airline experienced a high-magnitude AWS data breach compromising 6.5TB of data with over 23 million files being publicly exposed, including sensitive information like flight crew PII, plain text passwords, secret keys, and even source code.

Furthermore, despite the robust security measures in place by most cloud solution providers, businesses still have concerns about multi-tenancy, data sovereignty, and overall ownership of security.

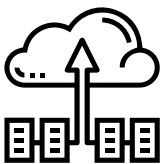
92%
of organisations
admit that they
have a gap between
current and planned
cloud usage and
the maturity of their
cloud security.¹

CYBER SECURITY COMPLEXITY IN THE CLOUD



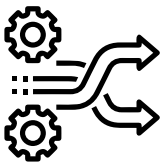
MIGRATION

Cloud migration can be complex and risky. Transferring large volumes of data and configuring access controls for applications across different environments creates significant exposure.



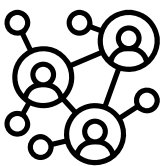
LEGACY SYSTEMS

Security and compliance issues with legacy systems stem from the lack of modern security features and can differ in their lifecycle and adaptability to the cloud – putting them at risk of cyber attacks.



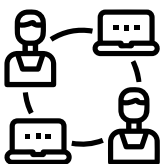
CONSTANT CHANGES

Without the right level of expertise or resource in-house, frequent new features and patches being rolled out by cloud providers can make it difficult for businesses to keep track of the constant changes.



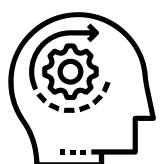
EXPANDING PERIMETER

It's easy to lose track of how an organisation's data is being accessed and by whom, since many cloud services are accessed outside of corporate networks and through third parties.



SHADOW IT

Many of the challenges around Shadow IT will only grow in the next few years as more enterprises adopt practices like BYOD, or more flexible remote work policies at the operational level.



TALENT AND SKILLSET

Cloud management and cyber security expertise have emerged as the highest-ranking organisation skills gap, which has been exacerbated by the pandemic.

Section four

WHAT KEEPS THE CISO UP AT NIGHT: THE MULTICLOUD SECURITY CHALLENGE

With businesses making the shift from on-premise to cloud environments, chief information security officers (CISOs) have had to adapt their security strategies to align with new technologies and processes and ensure IT employees have the appropriate skills to keep their organisations secure.

But it's typically not just a matter of switching from one on-premise data centre to one cloud service provider; CISOs also have to deal with the reality that enterprises often combine the use of multiple cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) for performance, scalability, and cost savings.

Given the growing complexity of systems and threats that come with moving to a cloud environment, and security policies that are unique to each provider, it makes sense that organisations are finding it increasingly difficult to secure the perimeter.

93%

of organisations have adopted a multicloud strategy.⁴

49%

of organisations cite multicloud security being a top concern.⁵

Common CISO challenges with multicloud adoption . . .

MISCONFIGURATIONS

IT employees don't understand multiple cloud environments and often make mistakes with security configurations.

VISIBILITY

Security settings, options, and tools are different for each cloud provider, preventing complete visibility in security analysis.

COMPLEXITY

Cloud providers have their own security standards and limitations with frequent features and patching updates.

DEPLOYMENT

The multicloud sprawl can lead to a fragmented approach to IT governance and security.

CONTROL

Data encryption and backups are not centralised, which can increase the risk of data breaches for businesses.

Section five

HOW TO REDUCE RISK IN A MULTICLOUD ENVIRONMENT

An organisation needs to unify the administration and monitoring of its IT systems. This means standardising policies and processes as well as the sharing of tools across multiple cloud providers. The challenge is to architect deployments that use native-cloud applications, when appropriate, while elevating security to work across all cloud environments to ensure migration and interoperability.

CONNECT POLICIES

Define and enforce a unified security policy configuration that connects all of the cloud providers your company uses.

CENTRALISE TOOLS

Consolidate security tools and identity and access management for IT staff and centralise data encryption.

AUTOMATE PROCESSES

Set up fully automated security audits, controls, patching, and configuration management.

DEPLOY CLOUD NATIVE

Use platforms that allow you to centralise your security configurations and management across environments.

WORK WITH SAAS

Use SaaS products to consolidate security policy, reporting, deployment, and other functions.

A shared responsibility model.

Variations in security controls from cloud to cloud further complicates matters, which is why security is a shared responsibility. What does this entail?

- 1 Understand SLAs:** When in doubt, refer to the master SLA. This can help avoid assumptions and misunderstandings that might leave security gaps or vulnerabilities.
- 2 Focus on data:** Consider classifying and categorising the data, and then implement security measures that are appropriate for each respective category while using stricter security measures for more sensitive data.
- 3 Manage credentials:** Who has access to what resources, services, and data? Use the tools offered by providers to help manage IAM and develop policies and processes to use those tools properly and consistently.
- 4 Consider tools:** Tools can provide automated correction for undesired security changes. Additionally, the right set of tools can help manage the noise and draw your attention to what's important.

Section six

THE FIVE PRINCIPLES OF CLOUD SECURITY

The NIST Cyber Security Framework provides standards, guidelines, and best practices for hardening your IT infrastructure. Based on risk-management processes designed to prioritise mitigation, these practices apply to cloud security as well.

The NIST framework centres around five core functions: **identify, protect, detect, respond, and recover**. When you're evaluating cloud security solutions, consider how well they score on these five functions.

»» IDENTIFY

You can't protect what you can't see, and you can't have an effective strategy if you don't understand your risks. You need complete visibility into your cloud assets and other elements, along with the ability to prioritise your risks.

Choose a solution that offers the capability to improve your visibility of asset inventory and risk assessment, amongst others.

»» PROTECT

A common challenge for security teams is the proliferation of tools that solve single, specific security problems. This makes it challenging to prioritise risks across the attack surface. It also leads to alert fatigue and results in ineffective security operations.

Choose a solution that provides a unified approach and consistency across your entire landscape.

»» DETECT

Providers typically offer 24x7 monitoring, but not all provide around-the-clock detection and response by experts. While automated tools and advanced tech such as AI are important, machines can't provide the critical thinking and analysis that humans bring to the table.

Choose a solution that incorporates the value you can only get from a team of experienced, threat-hunting experts.

»» RESPOND

Rapid response is critical—whether it be in response to a sophisticated ransomware campaign or an opportunistic cyber attack. Make sure you understand how your cloud security solution aligns with your mitigation workflows and processes.

Choose a solution that can support your ability to quickly contain an incident as part of an initial response.

»» RECOVER

Part of recovery involves building cyber resilience, which means not only being able to bounce back after a breach, but to bounce forward. As a result, you can minimise the likelihood, as well as the impact, of incidents that may occur in the future.

Choose a solution that can deliver a continually improved security posture for your business over time.

Section seven

TOP CLOUD SECURITY FEATURES AND FUNCTIONALITIES

Effective cloud security can fill the gaps in your talent shortage by removing the burden of protecting your cloud assets in-house. Since capabilities and features vary from provider to provider, make sure that the solution you choose works to achieve the outcomes your organisation needs.

Evaluate the comprehensiveness of the solution against the following features and functionalities.

1. IDENTIFICATION

- Identify assets across cloud platforms for visibility, reporting, and auditing purposes.
- Detect unauthorised cloud applications and services (shadow IT).
- Provide a single, integrated view of risks and threats across your cloud environment.

2. MONITORING

- Monitor, assess, and prioritise threats such as vulnerabilities and configuration changes.
- Monitor compromised SaaS credentials and suspicious user and admin behaviour and activity.
- Enable automated remediation and customised rules based on your environment.

3. OPERATIONS

- Bridge the gap between cloud-native security APIs and your team.
- Simplify your in-house operations with a solution that's easy to manage and maintain.
- Add value to your team with outside experts who can provide strategic guidance.

Cyber talent is a major cloud security challenge.

According to (ISC)2', the global cyber security workforce needs to grow by 65% to ensure that organisations have adequate protection against the growing array of cyber attacks that businesses face today.

Cloud security skills are particularly scarce, with 86% of companies experiencing a skills gap in this area according to 451 Research - especially as more organisations take advantage of cloud apps, multicloud, and hybrid-cloud strategies.

As cloud adoption continues to grow at pace, the skills gap in cloud security will only grow wider.

Section eight

ITC'S APPROACH TO CLOUD SECURITY

ITC's suite of cloud security services comprises of nearly 40 unique services (and growing). With our advisory-led approach, integrated delivery model and customer-first mindset, we are a long-term partner that can help you gain control of your cloud environment with the best combination of cloud-native security and human expertise.

»» ASSESS

Our approach to securing your multicloud starts with ITC's cloud security maturity model, an in-depth assessment that gives you complete visibility of your multicloud environment.

»» PLAN

Based on our assessment, a strategic roadmap will be developed to address your current and future risks covering the cyber security trifecta: people, technology, and governance.

»» DELIVER



In line with your roadmap, our cloud security experts deliver the right blend of cloud security solutions, overlay identity and access management permissions, and standardise your cloud environment, to enable your business to be 'secure from the start'.

»» MANAGE

In addition to delivering multicloud security solutions, you also gain access to ITC's unified suite of managed security solutions for continuous review and enhancements based on your changing requirements.

As a Microsoft Gold Partner with Advanced Specializations in Cloud Security, Threat Protection, and Identity and Access Management, we have the skills, knowledge, and processes to guarantee the highest levels of quality and reliability in cloud security.

ITC DELIVERED MICROSOFT MULTICLOUD SECURITY SOLUTIONS

Microsoft Defender for Cloud for the following workloads:			Microsoft Azure Cloud Remediations	Microsoft Entra Permissions Management
<ul style="list-style-type: none"> • Servers • App service • Azure SQL databases • SQL servers on machines 	<ul style="list-style-type: none"> • Open-source relational databases • Storage containers 	<ul style="list-style-type: none"> • Key vault • Resource Manager • DNS 	including but not limited to Azure PIM, Conditional Access, MFA, Storage Accounts, Subscription Permissions, PAM for SaaS apps.	including but not limited to multicloud identity health check.
<div> <div> Gold Microsoft Partner  </div> <div> Microsoft Advanced Specializations <ul style="list-style-type: none"> • Cloud Security • Threat Protection • Identity and Access Management </div> <div> Member of Microsoft Intelligent Security Association  </div> </div>				

Section nine

USE CASE: INTERNATIONAL TECHNOLOGY COMPANY IMPROVES ITS CLOUD SECURITY POSTURE WITH ITC

The customer

A leading cloud-based technology business that enables online remote support and collaboration globally for businesses and individuals who need remote desktop support, remote access, and online collaboration to connect worldwide.

The customer's cloud security challenge

- Reduced multicloud visibility.
- Multiple transformational projects in flight requiring burst resource.
- Expertise required to architect a holistic solution to adequately secure multiple vendor cloud privileged access.

The solution

ITC conducted an in-depth assessment of the company's cloud security posture against industry benchmarks and created a strategic roadmap that addressed and identified future risks covering the cyber security trifecta: people, technology, and governance, with special emphasis on identity and access management, for all the company's users across multiple cloud platforms.

As a Microsoft Gold Partner, with Advanced Specializations in Cloud Security and Identity and Access Management, ITC was able to provide specialist knowledge to remediate findings from the assessment. In addition, ITC was able to extend visibility, reduce operational costs, and decrease incident response times, leveraging a Zero Trust and Just In Time model to extend protections to multiple cloud platforms without increasing overhead on the security team.

ITC continues to support the customer on new cloud transformations and innovations to further secure the company's cloud journey.

The result

ITC's holistic approach, coupled with the robust security controls offered by Microsoft's Azure Platform, provided the customer with a solution that is flexible, expandable, and intuitive for admins and users alike.

As a result, the customer's security posture score has shown a positive improvement and they have gained access to additional cloud security skills that has enable them to secure their cloud journey today, and for the future.

Customer fast facts

- Global customer base
- Installed on billions of devices
- Has nearly 50 million devices online at any given time.

Cloud platform

- Public cloud hosted solutions, utilising Microsoft Azure, Amazon Web Services, and Google Cloud Platform.

ITC professional services solutions

- Multicloud framework compliance.
- Microsoft Azure Platform Remediations.
- Microsoft Sentinel.
- Multicloud privileged IAM.
- Licence optimisation with cost/risk.

Section ten

FINAL THOUGHTS

Organisations across all industries continue to leverage the dynamic efficiencies and scalability offered by the cloud. However, as cloud adoption continues to grow, so too will the gaps in cloud security.

If technology alone was the answer, the problem would have already been solved; yet 63% of organisations reported a breach in the last year, according to analyst firm Forrester.

The reality is that the effort, time, and expertise needed to navigate the complexity in creating a holistic cloud security strategy, as well as implementing that strategy to ensure visibility of a company's cloud environments, provides the right information to make an informed decision at the right time can be too time consuming on internal resources to deploy, configure, and maintain.

As a result, many organisations turn to managed security service providers (MSSPs) to remove the burden of deploying, configuring, and managing their security across multiple environments, including the cloud.

To stay ahead of the curve, it is essential that businesses take a holistic approach to cyber security, which goes beyond just pure technology. This means having the right approach and expertise to identify gaps in defences and implementing a strategy that considers the ever-changing landscape. It can be a daunting task, but with the right provider in place, it is possible to overcome the challenges and shift your cyber defence from a state of reactive to one that is proactive to keep your business safe.

The best security strategies are holistic, and cloud security is no different.

About ITC Secure

ITC Secure (ITC) is an advisory-led cyber security services provider and a Microsoft Gold Security Partner.

The company has a 25+ year track record of delivering business-critical services to over 300 global blue-chip organisations, bringing together the best minds in security, a relentless focus on customer service, and advanced technological expertise to help businesses succeed.

With its integrated delivery model, 24x7 fully managed state-of-the-art Security Operations Centre, and customer-first mindset, ITC works as an extension of its customers' teams to accelerate their cyber maturity – safeguarding their digital ecosystem and securing their business and reputation.

ITC serves global organisations from its locations in the UK and US with a world-class team of cyber consultants, technical designers, and cyber experts.

The company is a certified Great Place to Work® employer, active member of the Microsoft Intelligent Security Association (MISA) and winner of the Best Security Company of the Year 2021, Best Workplaces™ 2022 and Best Workplaces™ for Wellbeing 2022.

W: www.itcsecure.com | E: enquiries@itcsecure.com