Cyberfort

WHITE PAPER

Understanding and responding to the 5 biggest Cloud security challenges

WELCOME

White paper overview

In this article Cyberfort's Cloud and Cyber Security experts discuss the 5 most common security challenges organisations are facing when delivering their cloud strategy. It covers the major cyber security risks IT leaders need to be aware of and offers a range of recommendations of how to mitigate risk as part of an all-encompassing cloud strategy.

Introduction to the 5 biggest Cloud security challenges

Security in cloud computing has been a key consideration since cloud was first being adopted as part of an organisations infrastructure model over 10+ years ago. It is an issue many organisations are still having to adapt and evolve to as attackers become more sophisticated.

In their 2023 Cloud security study Thales discovered 39% of businesses experienced a data breach in their cloud environment last year, an increase of 4% from the previous year (35%) (1). This increase is down to a range of factors but is likely to get worse before it becomes better with Gigamon's 2023 cloud survey of IT Leaders finding 93% percent of global IT and Security leaders predicting cloud security attacks to increase in the next 12 months (2).

These increases are due to a range of factors but mainly include a lack of skills and resources to identify and respond to cyber-attacks on cloud infrastructure with Fortinet's 2024 Cloud Security survey reporting 93% of IT leaders are moderately or extremely concerned about having the right cloud security skills available to them (3). Add in the rise of AI powered cyber attacks on cloud infrastructure resulting in an estimated 75% of organisations having to rapidly adapt their cyber security strategy regarding cloud infrastructure according to Deep Instincts 2024 Voice of SecOps report (4). It is clear organisations need to start taking action to move from a reactive security approach in the cloud to a more proactive stance.

What are the 5 biggest Cloud security challenges?

As identified in the previous section of this article, cyber security and Cloud computing is still a hot topic. Security breaches in Cloud computing environments will continue to rise at pace if they are left unchecked and organisations do not have sufficient detection, response and proactive monitoring of Cloud environments in place. From discussions with our own customers and a variety of industry bodies Cyberfort believes the following 5 Cloud cyber security challenges should be on all IT leader agendas in 2024.

01 **Cloud cyber security models in a reactive state**

02 **AI driven threats now becoming more common in the Cloud**

03 **Phishing, social engineering, insider threats and privilege misuse**

04 **Changing regulatory frameworks and the impact on Cloud security strategy**

05 **Complexity in hybrid Cloud environments being exploited by attackers**

01 Cloud cyber security models in a reactive state

Traditional cloud cyber security models are in a reactive state in many organisations. As more pressure is being placed on cloud operating environments, organisations can no longer rely on a traditional approach to identifying and responding to attacks such as signature-based detection, manual monitoring and testing, historical detection and analysis and then post incident learning. Many of the traditional methods and cyber security models rely too heavily on manual interpretation of data and are simply not able to scale enough to deal with threats cloud computing is experiencing.

As cloud environments come under more pressure due to larger volumes of data being stored, processed and in transit, different types of users accessing the cloud and more and more applications relying on cloud accessibility and availability the cloud cyber security model needs to move to a proactive state.

So how can organisations put in place a proactive cyber security approach for their cloud environments?

Gain an understanding of the different clouds being used and what needs to be protected against specific threats. Start by identifying the data, applications and workloads in the cloud, then identify the potential risks of an attack. Compare and model the different attacks vs the risk profile of the organisation in terms of reputation, operational and financial impacts.

Be agile and adaptive to the cloud cyber security approach, start thinking like an attacker and assess where the most likely areas are for an attack. Don't just fall into the trap of thinking cyber security for the cloud is 'tick box' exercise. Proactively test and look to evolve your tactics to stop attackers.

Hunt for threats and vulnerabilities to identify the bad actors in your cloud environments, use AI tools and machine learning to recognise patterns of behaviours which attackers may be using. Look for the unknown vulnerabilities such as insecure software code or misconfigurations that are unique to your own cloud environment.

Adopt a 'zero trust' approach by understanding who is accessing your cloud. Make sure multi-factor authentication is in place, evaluate how best to restrict authenticated users access to only those areas of the cloud they need to do their jobs.

Make sure you have a focus on future changing regulations, the potential impacts on cloud security and test/trial new tools and techniques in relation to cyber security. Also review what is happening in other similar organisations and lessons you can learn to bring into your organisation for better cyber security management in the cloud.

Practice and test different attack scenarios. By testing and replicating potential attacks on the cloud, IT teams can quickly learn where they may be missing key skills and start to understand the potential impact on the organisation should an attack happen. By proactively testing and identifying gaps in cloud security plans can then be created to fill these gaps and incrementally improve cloud security over a period of time.

02 AI driven threats now becoming more common in the Cloud

Over the past 12 months many organisations have seen a significant increase in AI related cyber-attacks and threats. AI is increasingly being used by attackers for DDoS, ransomware and malware attacks which can adapt to the different environments extremely quickly. But it isn't just the traditional computing landscape which is being targeted by attackers. Many organisations cloud computing environments are coming under attack. According to Palo Alto's 2024 State of Cloud Native Report (5) 43% of CISO's believe AI powered threats in the cloud will not be detected by their traditional cyber security methods. The same report also found that 38% of CISO's viewed AI attacks on Cloud environments as their current number 1 cyber security concern.

So why is this the case? Quite simply attackers have realised that many organisations are suffering from having disparate data stored in a variety of locations as part of their cloud strategies. They also realise many organisations do not have enough skilled staff available to create and manage changing security policies for the cloud. It is also estimated that only 24% of AI tools being created and used in organisations as having a cyber security consideration as part of their build according to IBM (6). All of these factors are resulting in significant cyber security problems in the cloud as AI tools rely on data being generated, managed and stored in cloud environments.

Attackers are using AI tools to analyse human and machine targets in cloud computing, then generating code at a rapid pace to compromise organisations. The AI tools attackers are using can learn and adapt quicker than most humans and traditional cyber security approaches in the cloud are not able to keep up.

To overcome this cloud security challenge organisations should take the following steps:

Review existing cloud security tools and identify which events they are missing and/or are potentially missing from AI powered attacks. Understand which data could be compromised if an AI powered attack on your organisations cloud happens.

Identify where abnormal behaviours are occurring in the cloud operating environment. For example, review unusual login activities, access requests from a abnormal geographic regions or IP addresses, new user access requests, and changes in permissions on files and other resources, recent large data extraction and where increases in traffic may be happening.

Gain an understanding of your existing attack prevention capabilities in relation to AI powered attacks. Make sure you have the capacity and power to log users off, block accounts, isolate affected resources and have the right alerting systems in place for abnormal behaviour.

Invest in and make sure real time monitoring of potential attacks is in place. This will enable your organisation to respond in real time to attacks on the cloud infrastructure.

Use predictive analysis to analyse historical user behaviours vs what the future threats and the impact may be on your cloud environment if it is compromised. Then use this analysis to improve the security posture of your cloud environment.

Use a specialist 3rd party cyber security provider to undertake an independent assessment of your cloud security environment through pen testing. Use the reports generated to improve patch management and identify where manual intervention/specialist skills may be needed in the short term to ensure your cloud environment is secure.

03 Phishing, social engineering, insider threats and privilege misuse

Phishing, social engineering, insider threats and privilege misuse has come sharply into focus for cloud teams in the past 12 months. The reasons for this are because a wider range of employees are using the cloud for their daily job tasks than ever before. These 4 cyber security threats are not new for IT teams. As an example of the potential size of threat, it is estimated by Netskope that employees are 3 times more likely to fall for phishing scams than downloading a trojan horse for example.

It goes without saying if employees are accessing the cloud and clicking on phishing links, being socially engineered or misusing their access privileges then cloud computing in an organisation could be at serious risk of being compromised. In particular SaaS apps are most likely to be targeted as users access these on a daily basis to undertake their work. One Drive, SharePoint and Teams have all been highlighted as being major targets for attackers.

To mitigate these risks cloud teams should:

Look to direct employees to apps in the cloud only if they have a legitimate business reason for doing so.

Put in place education, training employees to be aware of the potential threats to the organisation and provide advice on how they can keep themselves safe.

Use intelligent tools and real time monitoring of what users are accessing in the cloud, implement a cloud security broker and create a data loss prevention strategy.

Assess insider threats and privilege misuse through behavioural analysis not just by job title. Understand what different users are accessing and if they are breaching their authorisation levels ensure they can be blocked or challenged as to why they are accessing data, applications or workloads in the cloud.

04 Changing regulatory frameworks and the impact on Cloud security strategy

Over the past 12 months many organisations have had to start planning for new regulatory frameworks such as DORA in Financial Services due January 2025, implementing the UK Governments pro innovation approach framework to AI which was launched in 2023, and keeping up to date with developments across PCI DSS, HIPPA, SOC 2, NIST 800-53 and 800-171, ISO27001 and GDPR. All these frameworks contain their own complexities in relation to how data is stored, managed and processed in the cloud.

To make sure your cloud security is ready to respond to changing regulatory frameworks consideration should be given to:

Reviewing data regulatory frameworks with upcoming framework changes identified. Then develop business cases for changing requirements in terms of storing, processing and transferring data in relation to cloud security.

Where your data is being stored in different clouds. Make sure the right security measures in place to protect data in different datacentre locations.

Review your Cloud Services Provider agreement and review their security arrangements vs different jurisdictions. If potential security gaps exist, develop a roadmap to close those gaps.

Understanding where skills gaps may exist in terms of understanding different changing regulatory frameworks and decide on whether to recruit or outsource for the skills required.

05 Complexity in hybrid Cloud environments being exploited by attackers

With it being estimated that over 79% of UK organisations having a hybrid cloud strategy (7) it is clear this is the main cloud operating model for most organisations. Security in Hybrid Cloud should not be underestimated. It is complex to manage and difficult to control due to the number and volume of components involved.

Many attackers have realised organisations with a hybrid cloud strategy could offer them 'rich pickings' due to the disparate nature of data being stored and moved between clouds, networks not being correctly designed to cope with hybrid cloud complexity, and gaps existing as organisations do not have the right skills available to proactively manage and monitor this approach to the cloud. From Cyberfort's interactions with a range of customers over the past 12 months we have identified the following security challenges as a high priority for organisations with a hybrid cloud strategy:

- Cloud vendor compatibility
- Data protection in terms of storage, processing and management in transit
- Network performance not up to standard with essential legacy equipment out of support and not being patched in a timely manner
- API's being poorly configured
- Compliance and risk management putting pressure on data management professionals who are focusing on other areas of cyber security and forgetting about the cloud
- Visibility and monitoring tools unable to assess security across the hybrid cloud environment

05 Complexity in hybrid Cloud environments being exploited by attackers

All these challenges require a unique approach and rely heavily on the right skill sets being available for IT Leaders to have confidence in their hybrid cloud security. To address these challenges, it is suggested cloud teams focus on the following areas to improve their hybrid cloud security:

Put in place the right cloud security posture management tools – These tools can help to automate risk management and ensure your organisation can meet compliance requirements. They help your cloud team to continuously monitor cloud systems for vulnerabilities and misconfigurations. Use AI to process threat data and take away potential human error.

Hybrid cloud must mean one hybrid identity – Organisations can use secure access service edge architectures or cloud access security brokers to monitor access and enforce security policies. Put in place authentication tools which have single sign on capabilities, so it is one identity per user. This will save the IT and security teams time in terms of monitoring cloud usage, make it easier to shut down log in ID’s who are displaying abnormal behaviours, better manage user privileges and enable an improved end user cloud experience.

Review if your organisation can move to a ‘cloud agnostic’ architecture – Many organisations are suffering from ‘cloud sprawl’ with different user groups using different clouds for siloed pieces of work. This in turn heightens security risk and can make a hybrid cloud infrastructure difficult to manage from a security perspective. IT teams should review the different cloud providers who make up their hybrid cloud environment and identify where consolidation in the cloud can take place. This will result in an improved security posture and easier overall management of users accessing the cloud and improved data management.

‘Zero trust’ approach embedded in the hybrid cloud environment – ‘Zero trust’ means thinking about everything in the cloud being a security risk. A true zero trust approach means strict user and device verification, management by implementing least privileges and assuming a network is already the network breached. This approach will help keep users safe and enable cloud security teams to identify and isolate problems in a targeted fashion.

Take advantage of AI and machine learning tools – Using machine learning and AI tools can enable cloud security teams to process large volumes of data on user behaviours, data access and assess the risk with different large volumes of data stored and managed in the cloud. They can help to identify the highest-priority threats from a range of security logs and can map them to attack patterns. This can help to focus security teams on the highest cyber security priorities in a complex hybrid cloud environment.

Cyberfort

SERVICES

Helping your business create, manage and deliver Secure Cloud services

Cyberfort Cloud

- Cyberfort's secure multi-tenant cloud
- Infinitely scalable
- Software-defined networking model
- Integrated backup included
- No ingress/egress charges
- Feature-rich optional native capabilities available

Private Cloud

- High performance dedicated platforms
- Compliant to regulatory & security requirements
- Proven technology stacks
- Secure UK Data sovereignty
- Tailored solutions
- Fully managed
- Certified engineers

Public Cloud

- Azure Managed Cloud
- AWS Managed Cloud
- Performance and cost optimised design & management
- Total cost of ownership calculations
- Build validation services
- Multiple billing options
- Flexible support levels from certified engineers

Hybrid Cloud

- Enterprise cloud
- Managed data protection
- Business continuity
- Managed connectivity
- Solution design
- Integrated platform with native Public cloud tooling and services

Cost certainty

Secure and compliant

Tailored cloud

High performance

Managed support

Skills on-demand

Cyberfort Secure Cloud Customers

ev qolcom DIGISEQ ADL SMARTCARE NEXUM™ B

Helping your business create, manage and deliver Secure Cloud services

Market-leading Technology Partnerships

Infrastructure, networking and connectivity

JUNIPER NETWORKS

Lenovo

DELL

FUJITSU

Platforms, data management and storage

Azure

vmware

aws

Microsoft

veeAM

NUTANIX

debian

Red Hat

kubernetes

ceph

Security and management

FreeBSD

elastic

HAPROXY

A10

Final thoughts

In this paper we have discussed the 5 biggest cloud cyber security challenges Cyberfort has witnessed in the past 12 months and what it believes will come into focus in the future. Managing cyber security in cloud environments is already complex and difficult to manage. One thing is clear. Now is the time for cyber security and cloud teams to start collaborating and developing the right security approach for their organisations cloud infrastructure so their data, systems, processes and people remain safe today and in the future.

1 https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release

2 https://www.gigamon.com/content/dam/resource-library/english/executive-summary/es-gigamon-hybrid-cloud-security-exec-summary.pdf

3 https://www.fortinet.com/blog/industry-trends/key-findings-cloud-security-report-2024

4 https://www.deepinstinct.com/pdf/voice-of-secops-5th-edition?submissionGuid=0621394b-f814-4095-8b70-93491f5e07f1 5

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/state-of-cloud-native-security-2024.pdf

6 https://www.techtarget.com/searchsecurity/news/366583496/IBM-study-shows-security-for-GenAI-projects-is-an-afterthought

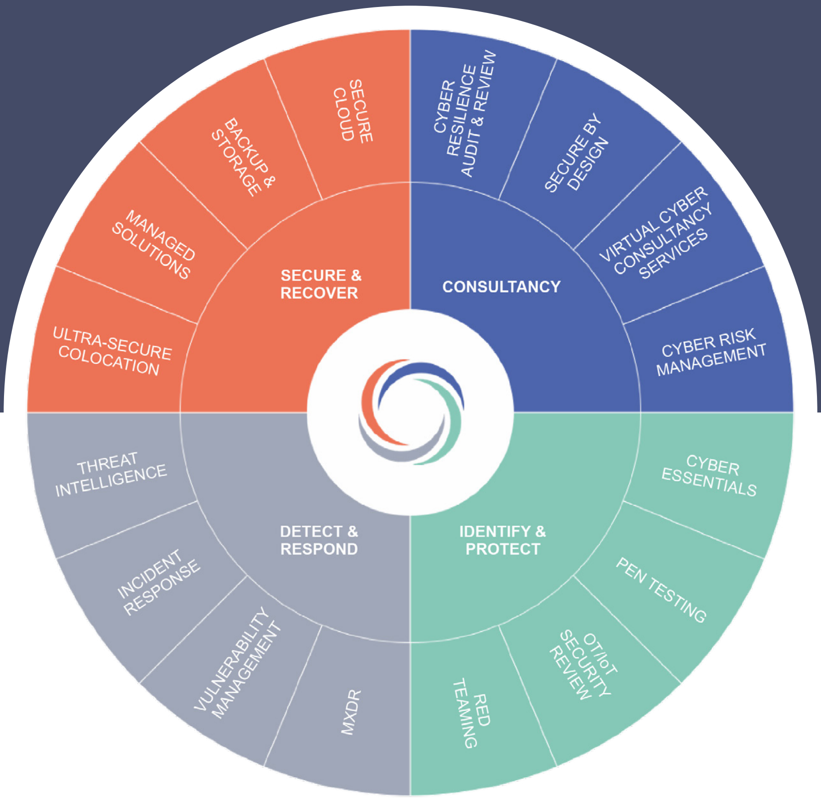
7 https://technologymagazine.com/articles/how-a-hybrid-cloud-approach-offers-the-best-of-both-worlds

Discover more about Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.



For more information on our Secure Cloud and Cyber Security services please contact us at the details below:
+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you