convergent

experts in the identification, assessment and mitigation of risk

'Insights' into Cloud Security

Part 1: How to avoid common cloud security issues

Executive Summary

This overview on "How to avoid common cloud security issues" is the first of an "Insights" titled series of informational documents. Focused on cloud and application security, our aim is to support our colleagues within Media and Entertainment to transition to the cloud and leverage its services securely. "Insights" will provide practical advice for large and small companies using SaaS, PaaS or IaaS cloud services whether already in the cloud or migrating to it.

In this paper we focus on how to avoid the common cloud security vulnerabilities by taking a methodical approach. Providing thoughtful insights on how to navigate the important strategic and operational challenges, we hope the information will assist those considering and planning for cloud deployments. For those already operating in the cloud the document will be the first step in assisting to establish internal assurance benchmarks in preparation for forthcoming external assurance requirements.

We believe that security should be forefront of all that you design and build for a cloud workflow to ensure a safe environment reduce the risks of a breach and prospect your business. In our opinion it's generally the same security issues that are the cause of all data breaches found in cloud environments.

Convergent's cloud security professionals have individual experience in undertaking security reviews over a wide cross section of sectors including, banking, insurance, managed service providers and media & entertainment.

Introduction

Where are you on your cloud journey?
The common misconception is that the cloud is secure by default. While this is true, the problem comes when cloud customers start applying their own configurations to workloads which then override the default security controls.

If you are using the public cloud already
Your IT team may have set things up organically without security input or consulting industry best practice or you may have been learning as you go without attending training courses. If you have taken this approach, it's likely that you may have security vulnerabilities that you're not even aware of. This white paper will help you to identify what the issues are and to provide some guidance on how to resolve them.

If you are beginning to migrate workflows into the cloud
This white paper will highlight key items that will help you to avoid making the common mistakes before you start your migration.

Shared Responsibility

Cloud is about a shared responsibility model. In on prem workflows all aspects of responsibility remain with the customer. If you are deploying virtual servers (IaaS) into the cloud, you as the cloud customer will be responsible for most of the security controls for these resources rather than the cloud service provider (AWS, Azure, Google etc.)

However, at the other end of the scale, if you are going to be using cloud native services (PaaS / SaaS) then the list of controls that you'll be responsible for will be much reduced. The diagram below shows who is responsible for what aspects of security within the standard deployment models:

It's essential that as a cloud customer, you understand what security controls you are responsible for and what the cloud service provider will cover before you start.

Common Cloud Security Issues

The table below summarises common security issues that can be avoided by the approach suggested in this document.

	Issue	Result
	Accidental Misconfiguration	Inadvertently exposing data
	Poor user identity management	Vulnerable to credential stuffing/ interception
	Poor vulnerability management	Systems have known vulnerabilities
	Insecure API configuration	Malicious access to content/data
	Lack of cloud security awareness	Inadvertently deploying cloud workloads with vulnerabilities
	Lack of adequate security monitoring	Malicious activity goes undetected

There are plenty of recent examples about high profile breaches and data breaches involving cloud workflows. Below we describe some typical examples.

Accidental Misconfiguration
Exposure of sensitive stored within public cloud can occur if the correct controls are not applied to the data. In addition, a lack of security monitoring will mean that this problem is unlikely to be detected in a timely manner. Education and cloud security awareness are also key here.

Ways to resolve:
1. Read the vendor best practice before deploying services into the cloud
2. Use Native cloud native security tools (Azure Security Center or AWS Security Hub and ensure that configuration alerting is enabled.
3. Implementing Identity and Access Management (IAM) correctly

Poor IAM implementation
Getting IAM right is a key element of effectively managing security within the cloud. Getting it wrong can lead to issues such as compromised credentials, inadvertent data access, for example where credentials are stolen, or an ex-employee still has access.

Ways to resolve:
1. Centralise identities e.g. use on premise Active Directory
2. Apply MFA to all user accounts
3. Implement role-based access.
4. Ensure authentication is required for all access
5. Follow vendor best practice for IAM

Poor vulnerability management
There are regular examples about stolen data where records of millions of people that personally identify them is exposed. This can happen when internet facing systems are not patched and hackers can take advantage of known vulnerabilities in order to access content.

Ways to resolve:
1. Ensure that all virtual servers are regularly patched
2. Ensure that a vulnerability management solution is implemented
3. Scan virtual servers & cloud services for vulnerabilities
4. Conduct penetration testing of web facing applications

Insecure API configuration
Data leakage caused by an API error often occurs through a badly configured API and is used by attackers to access client content.

Ways to resolve:
1. Configure API's in line with the cloud vendor's security best practice
2. Follow OWASP API top 10

Useful links on this topic are included below.

API Configuration Advice – OWASP API top 10
https://owasp.org/www-project-api-security/

Azure API Security Best Practice
https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-implementation

AWS API Gateway Security Best Practice
https://docs.aws.amazon.com/apigateway/latest/developerguide/security-best-practices.html

Lack of cloud security awareness
A high-profile case occurred in 2019 when internal source code and credentials were leaked onto the open internet which included software blueprints, access keys for a foreign exchange rate system, mobile application code and login credentials. This can happen when a GitHub code repository is left open to the public and can be compromised.

Ways to resolve:
1. Ensure that IT staff using cloud are adequately trained and aware of the typical pitfalls of using cloud or SaaS services.
2. Conduct regular education and training in cloud security for relevant staff
3. Centralise identity management for SaaS services back to the Identity provider for the organisation (in most cases this will be Microsoft Active Directory)
4. Ensure that MFA is used for SaaS services
5. Ensure that Access to SaaS services is integrated with your organisations JML process (joiners, movers and leavers)

Lack of adequate security monitoring
Personal data on millions of users can be compromised through which can happen when an attacker gains unauthorised accesses to your cloud environment. A lack of security monitoring and alerting across the cloud platform can result in common malicious activity patterns being undetected.

Ways to resolve:
1. Conduct active monitoring and alerting across the cloud platform
2. Deploying cloud native security tools if you don't already have a security monitoring and alerting solution

Security Considerations for Migration to the Cloud

1. Have clear objectives before you migrate to the cloud.
Ask yourself what you are trying to achieve:

- Creating a new base cloud environment ahead of the deployment of a specific workload?
- Deploying an additional workload into an existing cloud environment?

2. Attend the training first.
Attend training provided by the cloud service provider. Quite often this training is free and can be taken remotely using a self-paced approach. This will give you an insight into some of the basics. Links to training resources can be found in Appendix.

For Azure:
https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/
https://docs.microsoft.com/en-us/learn/certifications/azure-security-engineer

For AWS:
https://www.aws.training/Details/Curriculum?id=27076

3. Decide on a Migration Approach
Avoid the temptation to just lift n' shift resources into the cloud. Applying a traditional security approach to workloads in the cloud will likely leave you exposed. Further considerations include the following:

- Will your existing vulnerability management tool work in cloud? It's likely that you'll need an agent-based solution going forward due to the increased network segmentation in the cloud.
- Your threat landscape will continually evolve. Security misconfigurations must be considered in conjunction with infrastructure and application security in order to avoid vulnerabilities that can be exposed by attackers.
- Securing the admin console must be considered as it is now publicly available and no longer behind your corporate firewall.
- Remote access to servers might have been done from behind your firewall but in cloud, some additional thinking is required. Exposing your servers to the internet via SSH/RDP is not recommended.
- Do you currently allow untrusted systems to connect to your traditional IT systems? In cloud, you'll need to configure policies to prevent this happening otherwise all users will be able to connect from anywhere on any device.
- Will your existing security monitoring & alerting be able to interface with the cloud?
- Have you deployed the cloud agent required to collect security monitoring data?

4. Read the cloud service provider deployment guides before you start
Reading these will provide valuable insight. An example relating to best practice for IAM for Azure is below.

https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

Additional reference for best practice:

For Azure:
https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-design

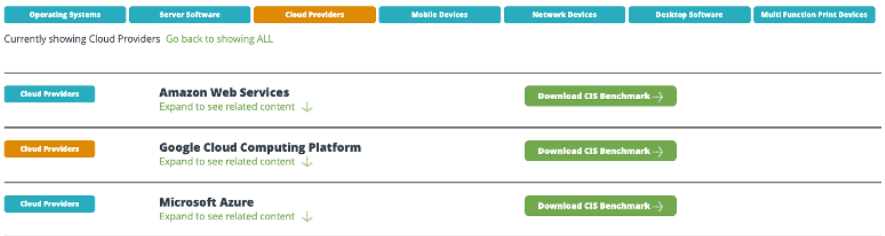
https://azure.microsoft.com/mediahandler/files/resourcefiles/security-best-practices-for-azure-solutions/Azure%20Security%20Best%20Practices.pdf

https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

For AWS:
https://wa.aws.amazon.com/wat.pillar.security.en.html

5. Read the 3rd party hardening guides before you deploy
Again, reading hardening guides will enable you to reduce the attack surface of your cloud workloads before you expose them to the world.

It's important to note that the hardening guidelines are not cloud agnostic and the correct guidelines must be followed. A link to the common security hardening guides for AWS, Azure and Google from the Center for Internet Security can be found in Appendix A.



6. Patching is still essential
If you are using cloud native services such as PaaS DB (MySQL, MongoDB, Azure MSSQL) then the cloud service provider will take care of the patching for you, however, If you are deploying virtual servers into the cloud, effective patching of these is a vital. Patch systems regularly and ensure your existing processes are updated to include cloud hosted virtual servers.

https://www.cisecurity.org/cis-benchmarks/

7. Consider deploying cloud policies to prevent security misconfigurations from happening
Security policies should be deployed into your cloud environment as this will help prevent the majority of misconfigurations from occurring.

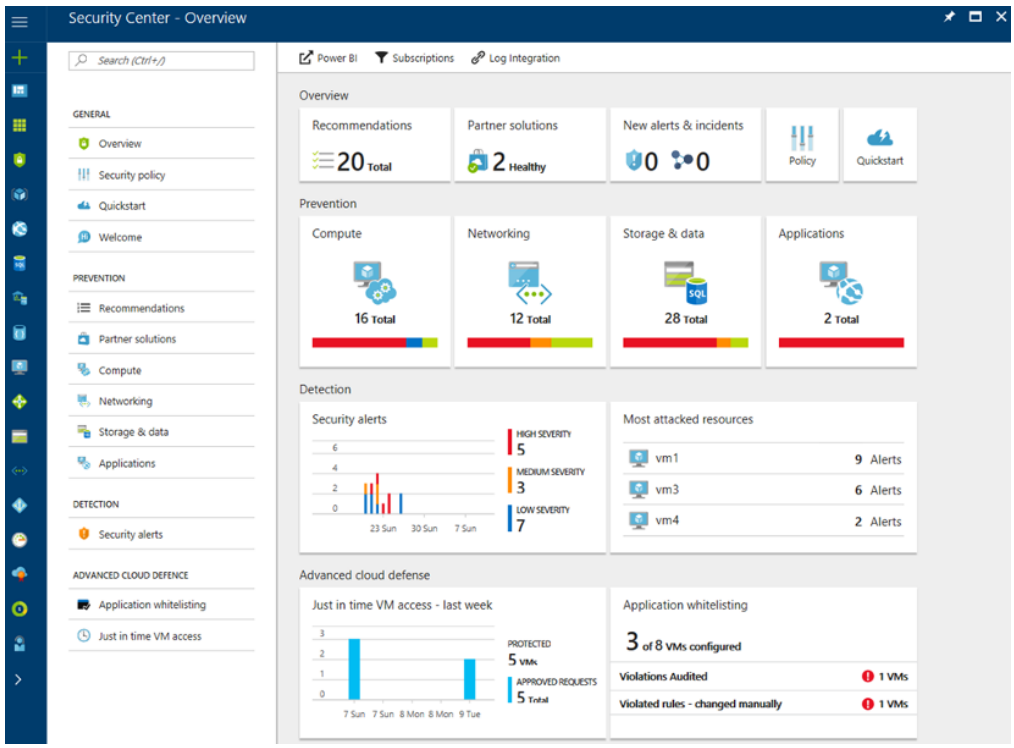
Links of how to do this in the common cloud platforms are included below:

For Azure:
https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage
https://docs.microsoft.com/en-us/azure/governance/policy/overview

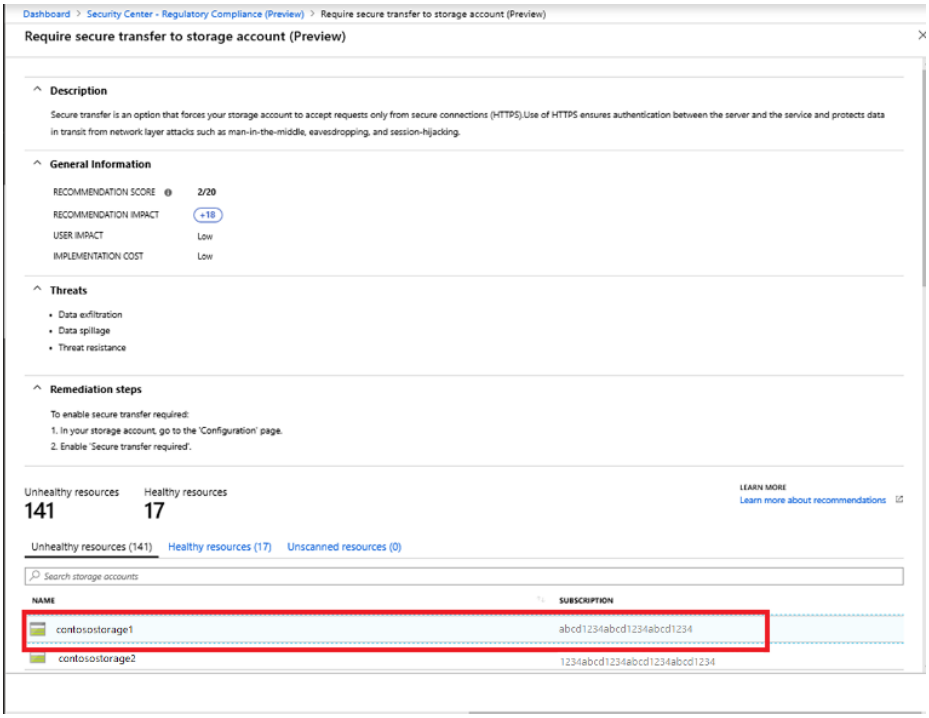
For AWS:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

8. Use the built-in security tooling
Continuous monitoring of your cloud environment is essential in order to quickly identify and remediate security issues. This can be easily achieved by deploying cloud native security tools For example in Azure, it's Azure Security Center. Azure Security Centre is a unified infrastructure security management system that strengthens the security posture of your data centres and provides advanced threat protection across your hybrid workloads in the cloud.

A screenshot of the console is shown below and a link covering how to get started with Azure Security Center is included in Appendix A [cross reference].



Azure Security Centre also provides guidance regarding how to remediate the issue…



For AWS, AWS Inspector is an automated security assessment scanner that can evaluate security loopholes and deviation from the best practices for applications hosted on AWS.

For useful reference information for both Azure and AWS, please refer to the links in below:

For Azure:
https://azure.microsoft.com/en-us/services/security-center/
https://docs.microsoft.com/en-us/azure/security-center/

For AWS:
https://aws.amazon.com/about-aws/whats-new/2020/04/aws-security-hub-launches-the-foundational-security-best-practices-standard/

9. Understand that the cloud is never still. Cloud Security is an ongoing requirement
In the traditional IT environment, it's likely that security audits take place annually but in the world of cloud, any change that you make is instantaneous. Can you afford to have vulnerability present for 5 days, 1 week or a month? – the chances are that the answer to this is no!

Organisations need to rethink security and ensure that they implement continuous security monitoring solutions to mitigate against this. These can be cloud native (e.g., Azure Sentinel) or third party provided (e.g., Splunk, Logrhythm and Alien Vault)

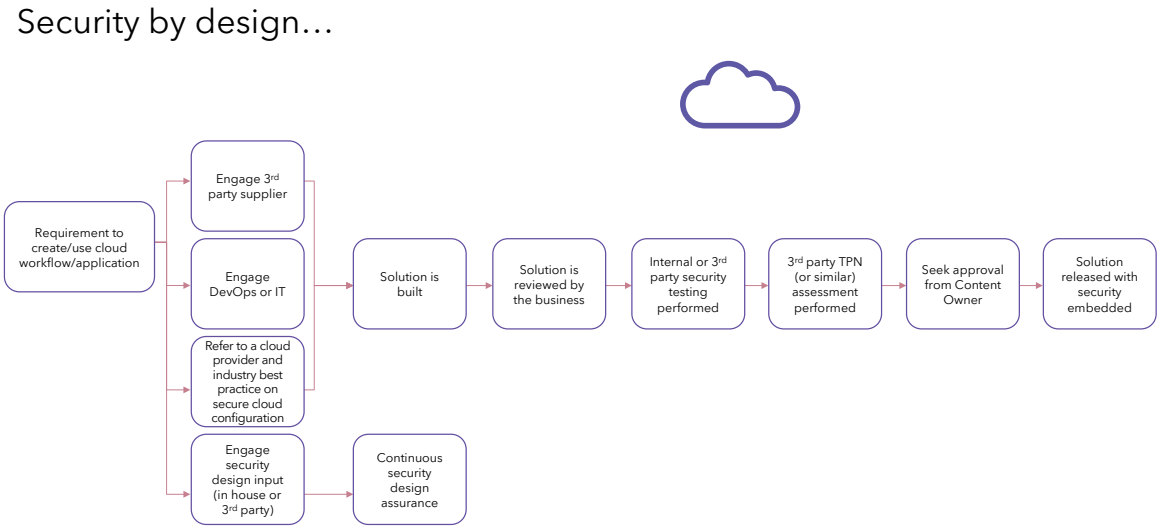
In addition, there are a number of companies offering managed security monitoring solutions.

Change is the new norm.

10. Recommended Security in Cloud Workflows

The following diagram shows a cloud workflow with a well-planned security strategy from the outset where security check points have been incorporated from the outset.

Cloud Workflow that is Secure By Design



11. Summary

Taking time before diving into cloud can save you pain of potential reputational and financial damage should things go wrong. Convergent is able to provide cloud security advice and guidance. Typically, it will cover the following scenarios.

- Assistance before embarking on a migration to cloud.
- Assistance during a migration.
- Assessing the security of a cloud environment/workload before seeking content owner approval.
- Security assessment as part of the content owner approval process.

Our cloud security professionals are able to undertake formal cloud security reviews for your organisation whatever your size and status by adopting a four-stage approach.

Stage 1: Discovery

We examine your cloud architecture and applications to gain an in-depth understanding to assess your current security status.

Stage 2: Security Governance & Mapping Against Best Practices

We review security governance and map your workflows against relevant industry best practice.

Stage 3: Review of Cloud Environments

We analyse all areas including virtual servers and plus network security and container workloads, patching and update policy, logging and monitoring, identity & access management, security hardening, code and key management. We identify potential gaps and weaknesses in security and areas in need of remediation.

Stage 4: Security Testing

We test against your stated security procedures including API security reviews and conduct penetration testing against OWASP Top 10 to highlight key areas of vulnerability and provide advice on hardening and remediation.

We Perform security testing against your environment. Example scenarios are:

- Testing that existing security controls are working correctly. (e.g. – do you have a WAF in place and will it stop common attacks? Will your security monitoring and alerting detect malicious activity?)
- Security testing of public facing API's (against the OWASP API top 10)
- Security testing of public facing applications (against the OWASP top 10)

We hope you've found this white paper a useful guide and welcome any feedback. Please contact us at:
info@convergentrisks.com

Offices in UK & US with global representation

www.convergentrisks.com

- TPN security assessments
- General assessments
- Penetration testing
- Vulnerability scanning
- Cloud security reviews
- Privacy compliance
- Management Portal

Appendix A

References

1. Shared Responsibility Model - Microsoft
   https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

2. The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-April2020 - Cloud Security Alliance
   https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven

3. Azure Identity and Access Best Practice
   https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

4. Azure Security Best Practice
   https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-design

   https://azure.microsoft.com/mediahandler/files/resourcefiles/security-best-practices-for-azure-solutions/Azure%20Security%20Best%20Practices.pdf

5. Azure security best practices and patterns
   https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

6. AWS security best practices
   https://wa.aws.amazon.com/wat.pillar.security.en.html

7. Hardening Guides
   https://www.cisecurity.org/cis-benchmarks/

8. Deploying Security policies into Azure
   https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

9. *https://docs.microsoft.com/en-us/azure/governance/policy/overview*

10. Deploying Security policies into AWS
    https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

11. Azure Security Center Overview
    https://azure.microsoft.com/en-us/services/security-center/

12. Azure Security Center Documentation
    https://docs.microsoft.com/en-us/azure/security-center/

13. AWS Security Hub
    https://aws.amazon.com/about-aws/whats-new/2020/04/aws-security-hub-launches-the-foundational-security-best-practices-standard/

14. AWS Inspector Overview
    https://aws.amazon.com/inspector/

15. Getting started with AWS Inspector
    https://aws.amazon.com/inspector/getting-started/

16. API Configuration Advice – OWASP API top 10
    https://owasp.org/www-project-api-security/

17. Azure API Security Best Practice
https://docs.microsoft.com/en-us/azure/architecture/best-practices/api-implementation

18. AWS API Gateway Security Best Practice
https://docs.aws.amazon.com/apigateway/latest/developerguide/security-best-practices.html

Training Resources

The training resources below are free for you to attend and are delivered remotely using the self-paced approach:

For Azure:
https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/
https://docs.microsoft.com/en-us/learn/certifications/azure-security-engineer

For AWS:
https://www.aws.training/Details/Curriculum?id=27076

Glossary:
IaaS – Infrastructure as a service
PaaS – Platform as a service
SaaS – Software as a service

Additional References:
The-Egregious-11-Cloud-Computing-Top-Threats-in-2019-April2020 - Cloud Security Alliance
https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven