CLOUD SECURITY

Organisations are storing the most amount of data we have ever stored online and in the cloud, and this will only increase as our dependence on Internet-based solutions grows moving from on-premise infrastructure.

Are your cloud solutions secure? Here are some things to consider when implementing cloud services...

1) Configuration

The efficiency of your business matters but it shouldn't come at the cost of reducing your security. Your default security posture should be considered at the most basic level and earliest stages of design and implementation of systems handling organisational data.

2) Encryption

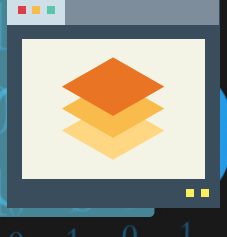
Use encryption, both on the server and during transmission to prevent personal and sensitive data being acquired in the event that your storage solutions are accessed by malicious actors. Encryption on the server isn't always turned on by default so time should be taken to ensure that encryption is enabled, particularly if services are being created dynamically through the course of daily business operations.

3) Role-based Access

The rule of least privilege should be deployed in every aspect; only allowing the minimum access of data to those who require it. Least privileged access means implementing rights to users that only provide the access they need and no more. Locking down permissions can be a complicated process but once you have your roles defined, template profiles can speed up the process in future.

4) Multiple Layers of Security

Multi-factor authentication (MFA) is an important consideration – it provides a low-cost and easy-to-implement additional layer of security between the user and accounts. Account compromises are often as a result of password issues making MFA a key component in securing systems and services.



5) Logging and Auditing

Logging and auditing doesn't just help to identify and record where things have gone wrong post-incident, they can also prevent a breach before an incident occurs or identify gaps to prevent potential issues in the future. Reputable web services have built-in tools for this such as the Amazon CloudWatch which acts as a monitoring service for IT managers. You can detect issues, visualise logs and automate remediation actions or notifications using these tools.