Fact Sheet

Cogito Group

Cloud Security Overview

The Benefits

There are many benefits to organisations, both large and small, gained from moving to the Cloud. There remains, however, fundamental issues around:

- Where is the data stored? (including back-ups).
- Who has access to the data?
- The possibility of insider threats.
- Jurisdictional overreach.
- The use of embedded encryption technologies.

These security vulnerabilities can be mitigated to ensure organisations can operate securely within the Cloud, with the understanding that they have full control and access over their data.

Traditional security tools aren't enough to monitor data moving to and from the Cloud, and between Cloud platforms. There are, however, several Cloud security tools that have been developed to address the challenges of maintaining control of your data in the Cloud.

Benefits of Moving to The Cloud

The Cloud offers many advantages over traditional on-premises solutions such as:

- Lower cost.
- Reduction in expertise required to manage these services.
- Geodiversity where this did not previously exist in an organisation.
- Ease of deployment.
- Ability to scale rapidly.
- Allows organisations to focus on core business, not the tools that assist in delivering core functions.
- Require less time consuming and costly implementations and maintenance activities.

Cloud Security Overview

Fact Sheet

Security Issues Moving to The Cloud

The Cloud however also presents some very real challenges to organisations around the security of the data stored there, such as:

- Data theft that causes:
  - A loss of IP.
  - Compromise of the commercial interests of an organisation. This can occur in private, commercial, or government contexts and can apply to such things as negotiations on the sale or purchase of products.
- Reputational damage through disclosure (e.g. the Sony hack).
- Data manipulation and compromise.
- Subjecting a person or entity to the laws of a foreign jurisdiction.
- The effective cessation of protections afforded to information by a local jurisdiction such as privacy and commercial disclosure laws.
- National security concerns where the services are to be used by Government or their contractors.

The prevalence of Cloud however presents several other challenges for organisations such as:

- The use of unapproved Cloud services (Shadow IT).
- The loss of data through disclosure to Cloud service (i.e. data that was never meant to be put in the Cloud).
- The loss of productivity through the overuse or unsanctioned use of Cloud service.

How Can Organisations Better Protect Common Cloud Services

Traditional security tools cannot optimally protect an organisations data in the Cloud. For example, they may not monitor data moving to and from the Cloud and between Cloud platforms. However, new and innovative Cloud security solutions have been developed to address these vulnerabilities, such as:

- Cloud Access Security Brokerage (CASB) which allows for organisations to extend their internal security policies to Cloud services. This gives their Cloud services similar levels of control over their data and access requirements that they would have for their internally hosted services.
- Encryption Services that cover both encrypting the data and the path, protecting the keys, BYOK, BYOE, HYOK, and Tokenisation.

Cloud Security Overview

Fact Sheet

Jellyfish CASB Capability

Next Generation Proxy Services

- TLS Decryption.
- Data Loss Prevention.
- Intrusion Detection System.
- Shadow IT discovery.
- Sanctioned IT usage.
- Analytics.
- UEBA.

Jellyfish Encryption Services

- Encryption Gateway Key Management.
- In Service Encryption.
- File & Folder Encryption.
- Virtual Machine Encryption.
- Database Encryption.
- Application Encryption (Cloud & On-Prem).
- Tokenised Encryption.
- Transfer Encryption.
- Key Encryption.
- Key Encryption and Diversification.
- BYOK & HYOK.

Jellyfish Identity and Access Management (IdAM)

- Provisioning, deprovisioning through SCIM.
- SSO.

Jellyfish CASB "Visibility" Services

- Analytics.
- Monitoring.
- Reporting.
- Log Storage.

Threat Detection Services

- Threat Intelligence.
- Malware Identification.
- Correlated activities analysis.

Incident Response Services

- Visibility over your interactions with Cloud services.
- Just in time education.
- Perform automated actions.

Configuration, Management and Control

- Policy Control.
- Jellyfish Admin UI.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, Cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.