CASE STUDY

HOW A AUSTRALIAN TELCO MAJOR ENSURED GOVERNANCE WITH TECH MAHINDRA CASB CLOUD SECURITY GOVERNANCE

BUSINESS CONTEXT

- Management and monitoring of compliance to Cloud Data Sharing policy
- Risk assessment of each service, detailed usage analytics, and Anomalous activities that presents risk to the organization
- Have a comprehensive view on cloud Service usage by analysing log information from egress devices (such as proxies, firewalls, SIEMs)
APPRAOCH AND SOLUTION

TechM’s approach and methodology involved:

- Setup Cloud access security broker along with existing BlueCoat Proxy Servers.
- Assign Data protection policies & Data Classification
- Support data masking to safeguard end user identity (Tokenization management)
- Integration with the SIEM solution to ensure timely alerts in case of non-compliance
- Configure various dashboards for Technical and CXO level teams to ensure management has a comprehensive visibility of organization confidential data being downloaded or uploaded.

IMPACT & HIGHLIGHTS

Efficient way to monitor cloud service providers being used by end users.

Protected The Consistent enforcement of security policies and usage of cloud.

Minimise the risk by installed malware via the unauthorised/unapproved software on the end points.

ESRM.Communications@TechMahindra.com

Copyright © Tech Mahindra 2021. All Rights Reserved.
Disclaimer. Brand names, logos and trademarks used herein remain the property of their respective owners.