AUJAS CYBERSECURITY

NSE NSEIT

CASE STUDY - CLOUD SECURITY

Cloud Security Enablement and Consumer Data Protection for the Second Largest Canadian Airline

CUSTOMER PROFILE

- Ninth largest in North America and Canada's second-largest airline.
- Operates an average of 777 flights and carries more than 66,130 passengers per day.

INDUSTRY

- Travel & Aviation

BUSINESS CHALLENGE

The client wanted to transition its existing on-premise data to the cloud. They were investing heavily in digital marketing platforms to drive growth and deserved a cloud data lake to foster operational efficiencies in marketing activities, grow revenue, and enrich customer experiences. They choose the Azure Cloud Platform to migrate their on-premise data. Azure helped them in having a scalable platform to meet the needs of a growing partner base and rapid rise in the number of business applications.

Though the cloud platform enabled business growth, it had security issues and challenges such as lack of data visibility, the absence in data control and compliance, inability to monitor data, lack of staff with skills to assess security gaps, and increased risk of data theft. These compromises on security could lead to non-availability of platform services, leading to financial and reputational losses.

SOLUTION RECOMMENDATIONS

Design and implement a complex, large-scale, multi-layered security architecture that can work across multiple protocols and applications.

Comprehensive defensive framework to secure the cloud platforms.

Build security from the beginning of the security architecture design stage.

SOLUTION APPROACH

- Design complex, large-scale, multi-layered security architecture and implement security controls and data protection of online data platforms. These platforms consolidate consolidates transactional and customer data, enabling marketing teams to mine big data and identify prospects for marketing campaigns.
- Real time monitoring of cloud platform and conduct penetration tests to keep the platform and customer data safe.
- Comprehensive defensive framework with built-in security from the beginning of design stage.
- Adopt secure SDLC process to enhance the security posture and speed-up deployments.
- Abide by Defense-in-Depth as a core security principle and implement multiple security controls to secure customer data. Advanced technologies & tools were deployed on the cloud through virtualized containers to ensure scalability.
- DevSecOps model to embed security controls and monitor the deployment cycle. Vulnerability Scanners, Continuous Integration and Continuous Deployment to deliver at speed along with effective vulnerability management.

SOLUTION HIGHLIGHTS

- Setup terraform templates to bring up the Inspec automation tool and deploy the benchmark profiles for continuous scanning, compliance and to measure the state of azure resources deployed by Ansible/Terraform.
- Voltage tool implementation for end-to-end data masking and encryption, including the protection of PII information used by data lake infrastructure.
- Configure custom rules to obfuscate data, while ensuring format preservation and usability to provide business context when consumed by BI applications.
- Ensure custom rule configurations helps the client to build data integration, drive data quality, establish data governance processes, and execute business intelligence & analytics use cases in a secure environment.
- Build capabilities into the solution to handle custom application rolling logs and devise processes to pass the logs to EventHub and be consumed by Jask tool.
- Implement security incident and event monitoring for the cloud platform and ensure continuous real-time monitoring.
- Raise alerts for unusual and fraudulent activities and ensure the team undertakes relevant actions.
- Perform threat modeling & architecture reviews of the platform to uncover any potential weaknesses to ensure these risks are known to the client and help them prioritize remediation measures.

CLIENT BENEFITS

REGULATORY COMPLIANCE

Mitigation of security issues in Azure Cloud Platform ensuring total compliance as per industry standards preventing the risks of hefty fines and losses due to non-compliance.

CLOUD AGNOSTIC

The security solution's cloud-agnostic approach allowed the client to adopt different cloud platforms across business lines and geographies. Cloud-agnostic security tools deployed for authentication, key management, vulnerability management, API, and containers helped the client in accommodating the migration needs of the future.

SCALABILITY

Virtual containers used to bundle applications could be scaled based on business needs, VM images using Inspec and registries secured by configuring baseline security controls.

ABOUT AUJAS

Aujas cybersecurity is an enterprise security service provider for organizations across North America, Asia Pacific, and EMEA regions. Aujas has deep expertise and capabilities in Identity and Access Management, Risk Advisory, Security Verification, Security Engineering & Managed Detection and Response services. By leveraging innovative products and services, Aujas helps businesses build and transform security postures to mitigate risks. The service focus is to strengthen security resilience by minimizing the occurrence of sophisticated attacks and threats while offering 360-degree visibility and protection across enterprise infrastructure.

For more information, do visit us at www.aujas.com or you can also write to us at contact@aujas.com