CASE STUDY – RISK ADVISORY SERVICES

Transforming the DLP Solution of a Large Multinational Bank into a Robust Security Asset

CHALLENGE

The bank with a vast global network of branches, remittance centers and ATM kiosks has been expanding rapidly over the past three decades and has won laurels for its exceptional online, mobile and customer center services.

To meet the growth in operational scale, the bank implemented a Data Loss Implementation (DLP) solution to meet regulatory compliance and security needs.

However, the solution had an inconsistent incident management process and did not align with security requirements. This slack in the solution also prevented the bank from establishing a database of sensitive data which could be accessed and updated by the bank's management.

The bank approached Aujas to transform the existing Data Leak Prevention (DLP) solution with a key focus to:

- Design the data protection governance and data leakage incident management framework to manage the consequences of data leakage more effectively and consistently.
- Assess more than 25 essential business functions to record sensitive data along with classification levels and data flow.
- Address structured and unstructured data.
- Establish a data repository for sensitive information accessed using DLP rules and allow bank representatives to maintain confidential information.
- Create and test DLP rules to protect repository data through a combination of keywords, RegEx, and fingerprinting techniques.

SOLUTION APPROACH

The engagement got executed in four phases:

- **Framework Design:** Create a framework for data protection governance and data leakage incident management for effectively managing the DLP solution. Ensure the framework has roles, responsibilities, processes, teams, responsibilities, communication plans, reporting and measurement metrics. Present the framework to the stakeholders for final approval and implementation.

- **Data Flow Assessment:** Identify business representatives and conduct workshops to orientate them on the need and nature of assessment. The representatives must capture sensitive data along with classification levels, compliance requirements and data flow across functions.

- **Data Repository Tool Rollout:** Design the tool workflow and develop the tool. Deploy the tool along with the sensitive document data captured during the assessment phase. Configure approvers and reminder notifications. Train business representatives on how to use the tool.

- **Rule Design:** Asses sensitive data to find appropriate ways of identification (keywords, RegEx, fingerprint). Create rules based on data flow. Test rules in monitoring mode, make the rules live and block low false positives.

BENEFITS

Established a robust DLP solution for continuous data protection.

Enabled the bank to identify data relevant for business use.

Maintain an updated repository of sensitive and regulated data.

Drive awareness of data protection among business functions.

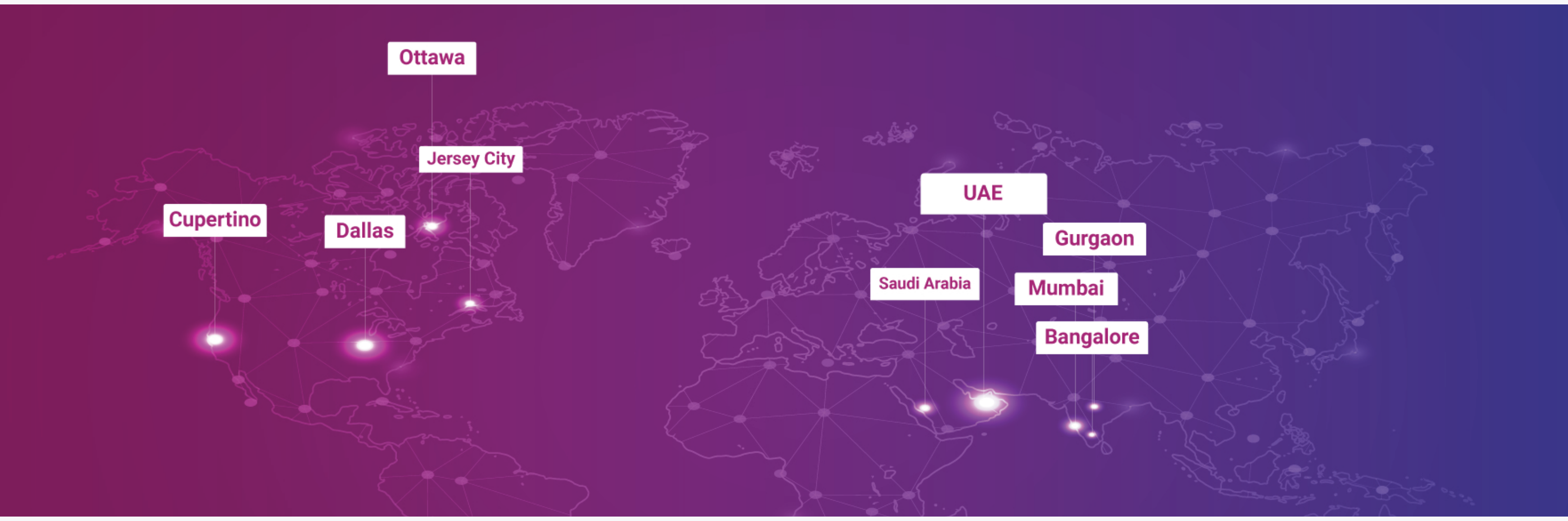
Managed data leakage incidents, filtered false positives.

Built rules for protecting data that matters.

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


Ottawa
Jersey City
Cupertino
Dallas
UAE
Gurgaon
Saudi Arabia
Mumbai
Bangalore