

CASE STUDY - DATA PROTECTION SERVICES

Design and Implementation of Data Leak Prevention Solution for a Large Retail Giant

CHALLENGE

The world's third-largest retailer with a global presence in 12 countries, having 6,600 stores and 6,000 plus employees, wanted to secure customer credit card information, customer and employee personal data, supplier details, strategy plans, and critical operational data. The enormous accumulation of data led to a rise in security risks, and it became increasingly important for the client to comply with PCI-DSS standards, and data privacy requirements to sustain customer trust and ensure market credibility.

The client wanted to ensure business users understand data sensitivity and take utmost care while using and sharing data. The challenge of this data protection initiative was to work with the business stakeholders to understand different types of sensitive data, where it is stored/used and how it is shared.

The retailer approached Aujas to design and implement a Data Leak Prevention solution to protect their data from leaks and breaches.

SOLUTION APPROACH

Our approach touched upon all elements directly involved or impacted by data.

- **Meet Stakeholders:** Create business-aligned DLP rules by involving key stakeholders, business unit leaders and their direct reports.
- **Identify Sensitive Data:** Recognize sensitive data, its location, storage and form, how it is moved within and outside the organizational environment.
- **Foster Culture Change:** Ensure business users understand the criticality of information and the reason to safeguard data from leaks through workshops.

- **Create DLP Rules:** Standardized templates were used to capture data structure/lifecycle and develop DLP rules for discovery and leakage monitoring. Enable the DLP solution to recognize information using methods such as fingerprinting, keywords, etc.

The solution was implemented in four phases:

Strategy Definition:

- Define governance structure, roles, and responsibilities.
- Create an interaction model for communication among various stakeholders.

Data Flow Analysis:

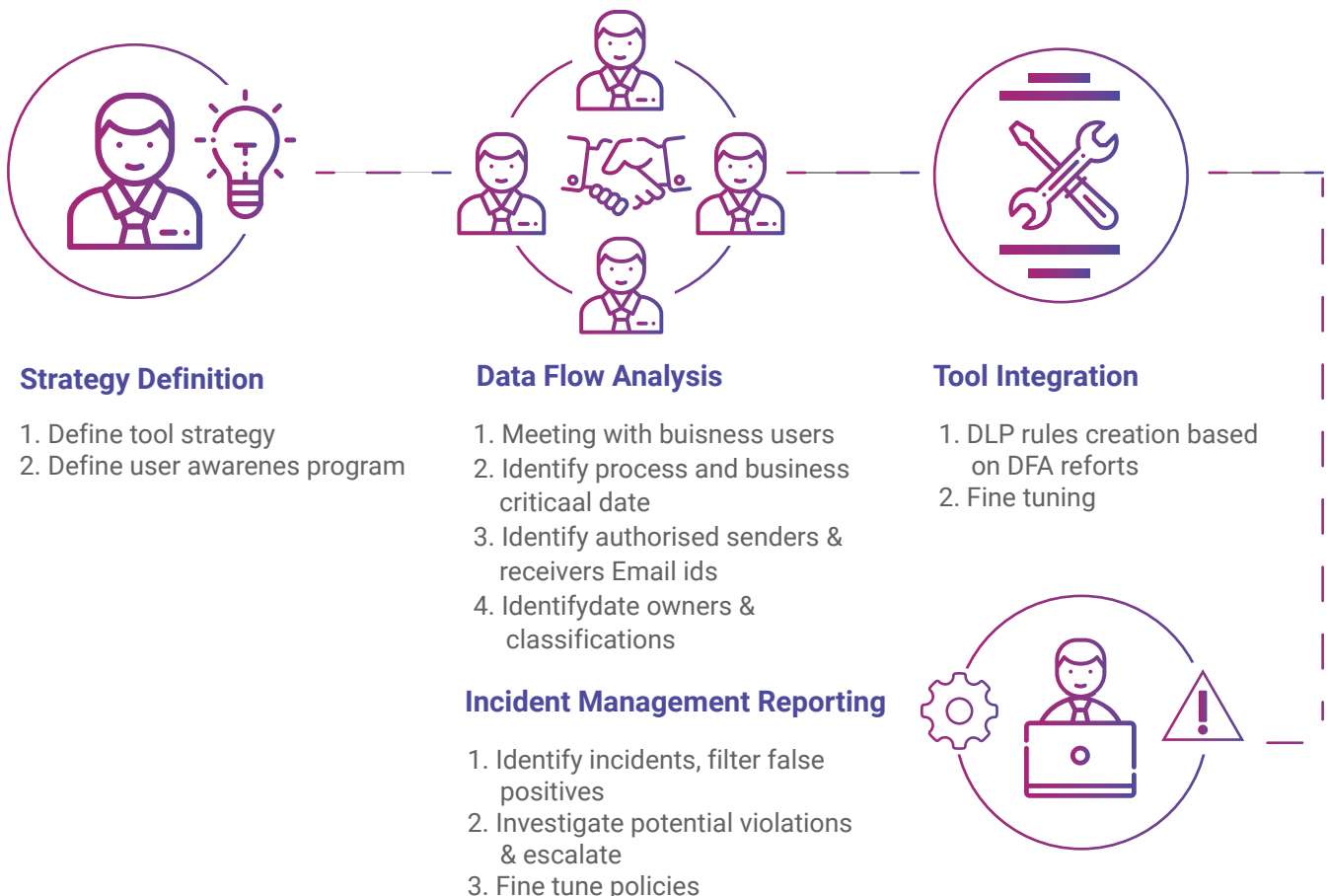
- Analyze business processes and identify data leak and exposure points.
- Perform data flow analysis to identify critical information, its flow within & outside the organization, information owner details, keywords to identify documents, and authorize sender & receiver email ids.

Solution Implementation (DLP Tool Integration)

- Implement DLP solution and create rules for data protection based on the data flow analysis report.

Sustenance (Incident Management & Reporting)

- Establish new and customized policies, fine-tune the policies after monitoring them for two weeks.



BENEFITS



Exhaustive catalog on sensitive information and data flow processes for the client.



Customer and employee data flow to personal email ids monitored and protected.



Round-the-clock data monitoring to ensure the right data is shared with the right people.



Provide on-demand reporting for decision support, management team, and auditors.

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

You can also write to us at contact@aujas.com

