

## CASE STUDY – RISK ADVISORY SERVICES

# Design and Implementation of an Advanced DLP Solution for a Large Insurance Firm

## CHALLENGE

The insurance provider has an extensive portfolio of offerings ranging from auto, health, property, and casualty insurance services. To safeguard information and meet regulatory compliance requirements, the company implemented the ISO27001:2005 controls. They now wanted a DLP solution to enhance information security and privacy controls.

### Key challenges included the need for:

- Data protection governance and data leakage incident management framework to manage the consequences of data leakage incidents.
- Data flow analysis across 20 business functions and record data with classification levels.
- Identifying and implementing the appropriate DLP technology by selecting a technology vendor who can understand the insurance firm's core business applications & assets and detect data leakages in them.
- Creating and testing DLP rules through a combination of keywords, RegEx, and fingerprinting techniques before making them live.
- Identifying incidents, remove false positives and work with internal teams to manage data leakage incidents.
- Fine-tuning and optimization of DLP implementation to ensure better alignment with business data movement rules and KPI reporting format

## SOLUTION APPROACH

### The project execution consisted of four phases:

- **Framework Design:** The framework consisted of roles and responsibilities, processes, team responsibilities, communication plans, reporting, and measurement metrics.
- **Data Flow Assessment:** Identify business representatives and conduct workshops to orientate them on the need and nature of assessment. Train them on how to capture structured and unstructured data by following classification levels, compliance requirements and data flow across business functions. Assess sensitive data to identify the appropriate means of identification, such as keywords, RegEx, and fingerprint.
- **Rule Design:** Create rules based on data flow. Test rules in monitoring mode. Make the rules live and block low false-positive rules.
- **Incident Management:** Monitor DLP incidents. Filter false positives, identify trends and streamline rules to confirm incidents. Assess incidents for escalation & coordinate accordingly. Provide periodic KPI reports to management.

## BENEFITS



Established the DLP framework for continuous data protection.



Identification of relevant business data.



Assisted the client in selecting an appropriate DLP solution.



Built rules for protecting critical data and implemented them.



Managed data leakage incidents and filtered false positives.



Reports on Key Performance Indicators of DLP solution to executive leadership.

## 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](http://www.aujas.com) or you can also write to us at [contact@aujas.com](mailto:contact@aujas.com)

