DATA LEAKAGE PREVENTION

INDUSTRY – BFSI

DOYEN
LEVERAGING TECHNOLOGY.
ENABLING BUSINESS

Introduction

Stringent regulatory and compliance standard as forcing today's IT Teams are straddled with the responsibility of ensuring data protection and safety at all costs. However, this is becoming increasingly complex task due to growing data volumes, remote and mobile users. Users often try to pilferage data using unauthorized removable storage devices, USB pen drives, web uploads, E-Mail attachments, print outs and so on.

The customer, one of India's largest leading financial services group with operations that span more than 40 different line of businesses and subsidiaries. With growing business opportunities, customer too faced challenges in securing and protecting their data.

KEY CHALLENGES

- Prevent use of **unauthorized storage devices.**
- **Discover and Classify** data
- Protection against data leakage and theft
- **Management Complexity** of DLP solutions

SOLUTION FEATURES

- **Automatic and Granular Data Classification**
- **Granular control** with user and device based policies
- **Data Leakage Protection** through different channels
- **FIPS and Common Criteria certified** military strength encryption algorithms.
- **Detailed logging and Incident reporting**

DOYEN's Solution

After evaluating a number of different solutions, DOYEN deployed McAfee Total Protection for Data as a solution for the customer to provide a unified and centralized architecture that combines Host DLP, Drive encryption and File and Folder encryption modules. It allowed for granular data classification based on application, location and content of data. The DLP module helped monitor, block and prevent data leakage. In addition, detailed logs provided forensics to generate incidents.

The solution helped the customer mitigate risk of intentional or accidental Data leakage and loss.

Outcomes and Benefits

The customer has granular control over data leakage channels and can hold every staff member accountable. Military strength encryption ensured data protection in case of device theft or loss. In addition, user and device based policies were possible for granular deployment.

To learn how we can help write to us at ***info@doyeninfosolutions.com***