Building a Secure Data Foundation: Azure Solutions for BFSI & Public Sector

This guide explores how Azure helps BFSI and Public Sector organizations establish robust data governance and classification, building a secure foundation for sensitive data.

Prepared by:

Muppina Jeevan Teja Swamy

Job Application Developer at IBM (Hyderabad)

Table of Contents:

1.Introduction:

In the ever-evolving landscape of data management, industries such as BFSI and the Public Sector face unique challenges in safeguarding sensitive information. Microsoft Azure, a comprehensive cloud computing platform, offers robust solutions to address these challenges.

BFSI and Public Sector:

The BFSI and Public sectors manage a treasure trove of sensitive data: financial records, personal information, and classified documents.

Figure 1 BFSI

Failure to secure this data leads to:

- Financial losses: Fraudulent transactions, data breaches, and regulatory fines.
- Reputational damage: Erosion of trust, public backlash, and loss of business.
- Operational disruptions: Data inconsistencies, errors, and hindered decision-making.

Building the Case:

- Current data management practices often fall short: Manual processes, siloed data, and outdated technologies leave vulnerabilities.
- The need for a new approach: Standardized and automated solutions are crucial to strengthen data security.

Introducing the Hero:

Enter data security solutions for BFSI and Public sectors: Automation, encryption, AI-powered anomaly detection, and robust governance frameworks.

These solutions help:

- Prevent data breaches: Proactive identification and mitigation of threats.
- Ensure compliance: Adherence to strict regulatory requirements.
- Enhance data quality: Accurate, consistent, and readily available data.
- Unlock new insights: Leverage data for better decision-making and innovation.

Microsoft Azure

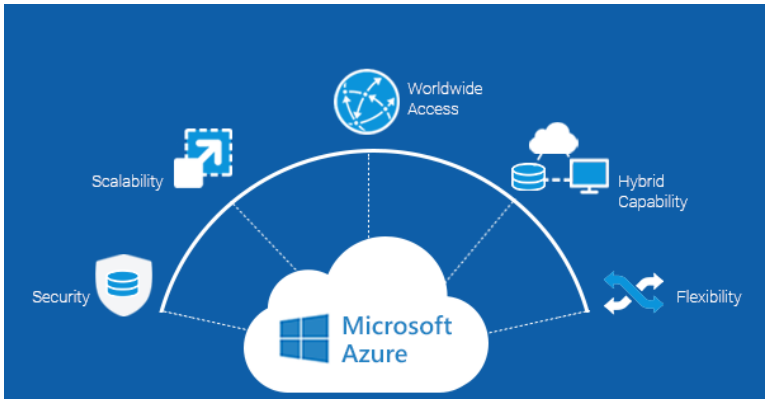

Figure 2 Microsoft Azure

Azure serves as the backbone for modernizing data management in the BFSI sector and the Public Sector. Its diverse set of services provides a foundation for building secure, compliant, and scalable solutions.

- **Azure Information Protection**

Azure Information Protection (AIP) takes centre stage in data classification. By enabling organizations to label and protect their data, AIP ensures compliance with regulatory standards and strengthens data security.

- **Azure Purview**

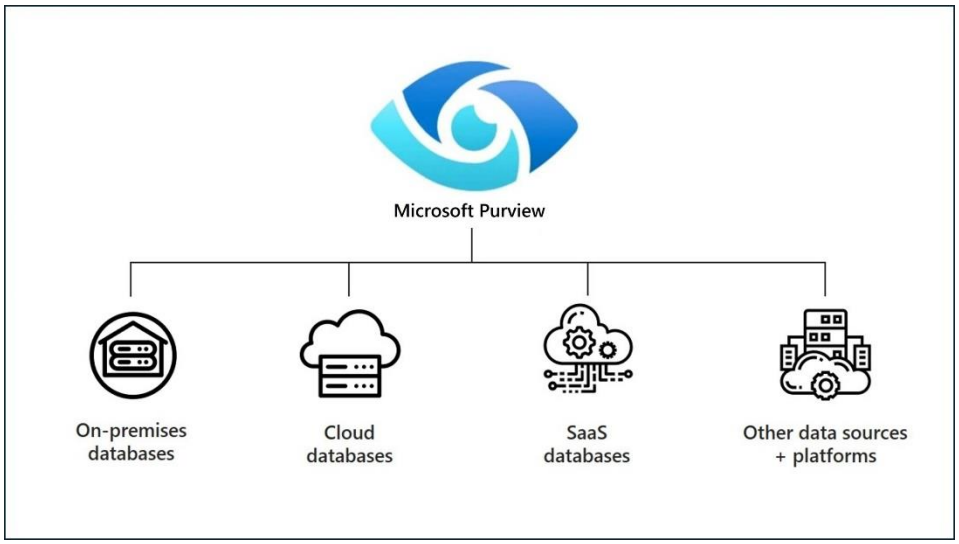

Figure 3 Azure Purview

Azure Purview acts as a unified data catalog, simplifying the discovery, understanding, and classification of data across diverse sources. This powerful tool streamlines data management, fostering transparency and efficiency.

- **Common Azure Features**

Understanding the core features of Azure, including the Azure Portal and Azure CLI, is essential for effective implementation and management of data governance solutions.

2.Problem Statement

In the BFSI sector and the Public Sector, the handling of sensitive data poses significant challenges. The absence of a standardized and automated approach often leads to compliance issues, data breaches, and difficulties in maintaining data quality.

- **What is the Solution?**

To address the challenges faced by the BFSI sector and the Public Sector, a standardized and automated solution is imperative. This solution lies in the strategic implementation of Azure Information Protection and Azure Purview.

- **The Need for a Standardized and Automated Solution**

A standardized and automated approach ensures consistency, efficiency, and adherence to compliance requirements. It becomes increasingly critical as the volume and complexity of data continue to grow.

3.Solution/Architecture

Azure Information Protection (AIP) for Data Classification:

Configure AIP labels

Figure 4 Configure AIP labels

In the Azure portal, navigate to the Azure Information Protection service. Define sensitivity labels, such as **"Confidential"** and **"Internal Use Only"**

Apply Labels Programmatically

Utilize the Microsoft Information Protection SDK to programmatically apply sensitivity labels to files. Here's a simple Python script using the SDK:

```python
from mip import LabelingOptions, FileEngine
from mip.data import ContentLabel, Sensitivity

file_path = "path/to/your/file.txt"

options = LabelingOptions(content=ContentLabel(sensitivity=Sensitivity("Confidential")))

with open(file_path, "rb") as file:
    labeled_data = FileEngine().label_file(options, file.read())
    with open("path/to/your/labeled/file.txt", "wb") as labeled_file:
        labeled_file.write(labeled_data)

```

Figure 5 apply sensitivity labels

Azure Purview for Data Discovery

Set up Azure Purview

In the Azure portal, create an Azure Purview account. Configure metadata definitions, and set up scanning configurations for various data sources.

Scan and Classify Data

Initiate a scan using PowerShell to automate data discovery and classification within Azure Purview:

```
$accountName = "YourPurviewAccount"
$resourceGroupName = "YourResourceGroup"
$scanName = "YourScan"

Start-AzPurviewAccountScan -AccountName $accountName -ResourceGroupName $resourceGroupName -ScanName $scanName
```

Figure 6 Scan and Classify Data

4.Technical Details and Implementation:

Azure Information Protection (AIP):

-Integration with Microsoft 365 Apps:

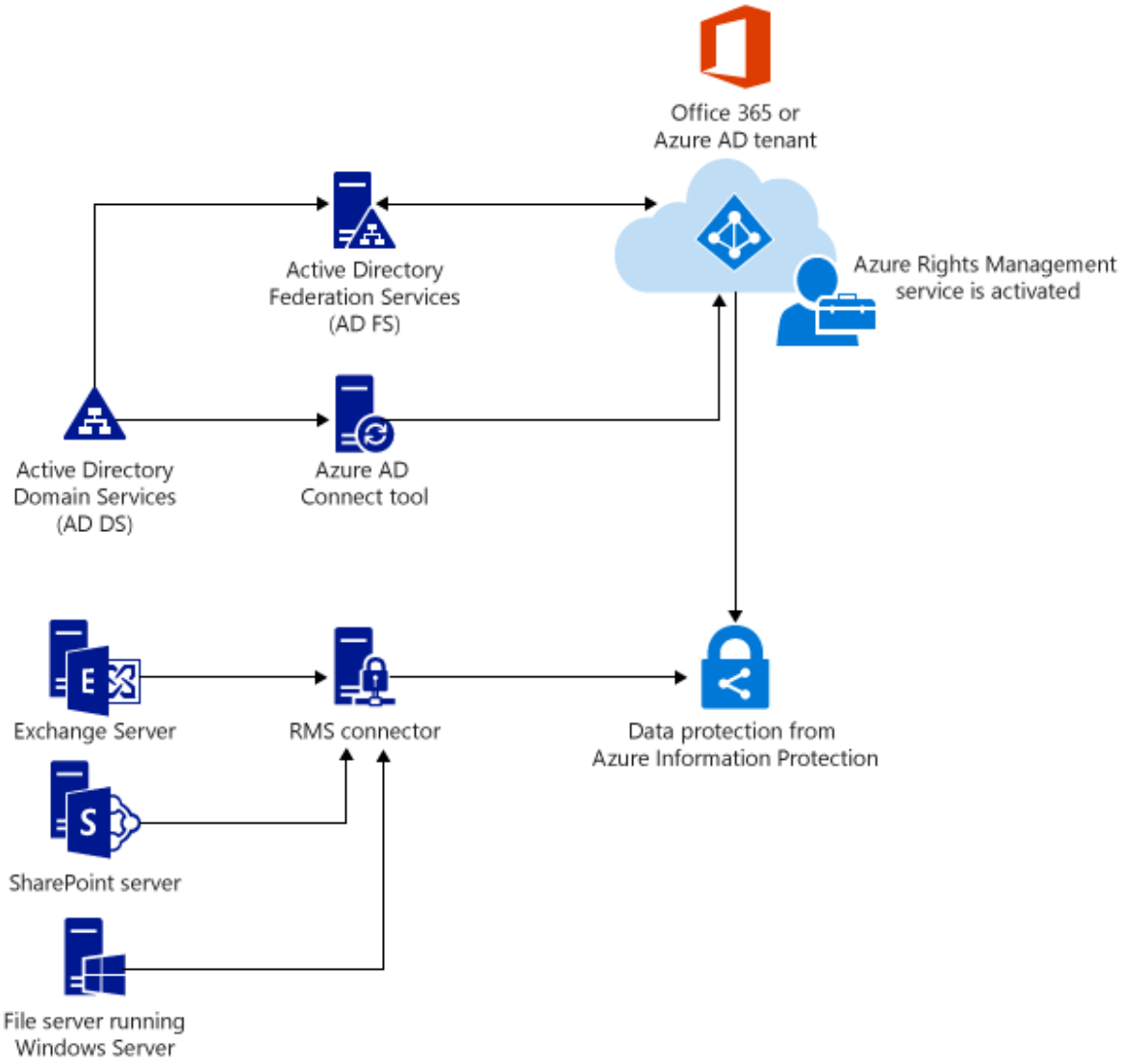

Figure 7 Integration with Microsoft 365 Apps

AIP seamlessly integrates with Microsoft 365 apps. Users can classify and protect documents directly within applications like Word or Excel.

-Programmatic Labeling with SDK:

Utilizing the Microsoft Information Protection SDK, developers can programmatically apply sensitivity labels. This ensures consistency across various applications and data processing workflows.

```
# Code snippet for programmatically applying sensitivity labels using the SDK
# (This code assumes that you have the necessary SDK installed)
from mip import LabelingOptions, FileEngine
from mip.data import ContentLabel, Sensitivity

file_path = "path/to/your/file.txt"

options =
LabelingOptions(content=ContentLabel(sensitivity=Sensitivity("Confidential")))

with open(file_path, "rb") as file:
    labeled_data = FileEngine().label_file(options, file.read())
    with open("path/to/your/labeled/file.txt", "wb") as labeled_file:
        labeled_file.write(labeled_data)
```

Figure 8 apply sensitivity labels

Azure Purview:

-Unified Data Catalog:

Azure Purview provides a centralized catalog for discovering and understanding all data assets within an organization, promoting transparency and accessibility.

-Automated Scanning and Classification:

Purview's automated scanning capabilities identify sensitive data, ensuring proper classification based on predefined policies. The PowerShell script initiates a scan to automate this process.

5.Challenges in Implementing the Solution:

-Integration with Existing Systems:

Integrating AIP and Purview with existing data storage and processing systems.

We can conduct compatibility testing, refer to Azure's documentation, and leverage support resources. https://learn.microsoft.com/en-us/azure/

-User Adoption and Training:

Ensuring end-users and administrators are proficient in using AIP labels and understanding Purview scanning processes.

-Data Volume and Velocity:

In industries dealing with a high volume of data transactions, such as BFSI, managing the velocity and sheer volume of data can be challenging. Real-time data governance and classification require scalable solutions to handle the continuous influx of information.

6.Business Benefits:

-Regulatory Compliance:

AIP and Purview assist organizations in meeting regulatory requirements, crucial for the BFSI sector and the Public Sector.

-Data Security and Risk Mitigation:

By classifying and protecting sensitive data, organizations can significantly reduce the risk of data breaches.

-Efficient Data Management:

Automated data discovery and classification streamline data management processes, allowing organizations to efficiently organize and utilize their data assets.

-Scalability and Future-Readiness

Azure services provide scalability, allowing organizations to seamlessly adapt to the growing volume and complexity of data. Future-proofing data governance practices ensures that the organization remains agile and prepared for evolving regulatory requirements.

-Streamlined Compliance Audits

Regular compliance audits are simplified with standardized data governance practices. The ability to showcase well-defined data classification and protection measures streamlines the auditing process, ensuring swift compliance assessments.

-Customer Trust and Privacy Compliance

In BFSI and the Public Sector, where customer trust is important , robust data governance instills confidence. Compliance with privacy regulations, such as GDPR or HIPAA, becomes more manageable, reinforcing the organization's commitment to data protection.

7. Conclusion:

In conclusion, the practical implementation of data governance and classification using Azure Information Protection and Azure Purview provides a robust solution for the BFSI sector and the Public Sector.

By these tools, organizations can ensure compliance, enhance data security, and efficiently manage their vast datasets.

As industries continue their digital transformation journey, Azure's capabilities become pivotal in building a secure, compliant, and data-driven future.