## User Story 5 – Data Storage, Secrets & Observability

As a Platform Engineer,

the objective is to ensure that data storage, secrets,
and system monitoring are handled in a secure and centralized manner so that
the platform remains reliable and observable.

Service attachments are stored in Azure Blob Storage instead of Dynamics 365. Only metadata and references are maintained in CRM. This approach reduces CRM storage usage and improves performance while keeping attachments easily accessible when required.

Secrets such as connection strings, API keys, and access tokens are stored in Azure Key Vault. Applications and services access these secrets using managed identities, ensuring that no sensitive information is hard-coded or exposed.

System observability is implemented using Azure Application Insights. Logs are captured for workflow executions, function runs, and failures. Metrics such as execution time, failure count, and request volume are monitored to identify performance or reliability issues.

Alerting is configured for critical scenarios such as repeated automation failures, SLA breach spikes, and storage access issues. These alerts help ensure that problems are detected early and addressed promptly.

**Limitations and Trade-offs:**

Using Blob Storage introduces eventual consistency, and extensive telemetry collection in Application Insights can increase monitoring costs. These trade-offs are managed through retention policies and selective logging.

**Automation Flow Diagram :**

Users
Azure AD / Azure AD B2C
Dynamics 365
SSRS
Power BI
Azure Logic Apps
Azure Functions
Azure Blob Storage
Azure Key Vault
Application Insights