LTIMindtree

Brochure

LTIMindtree Maskot
Data Protection Solution

Rapid adoption of automation and cloud technologies across enterprises has led to data proliferation, making data more prone to vulnerabilities and breaches. The increasingly complex IT environment deploys this data to develop data sets for test, development, and training purposes, as well as onsite or remote backups. In production support, various day-to-day operations like file triaging and data sharing, pose a risk of PII exposure in unauthorized environments. Additionally, global enterprises have multiple data collection points ranging from campaigns, cookies, to surveys, and employee data. The data from all these sources is moved across multiple systems and shared with third parties such as vendors, regulators, etc. thus increasing the risk exposure.

LTIMindtree has developed a platform – Maskot which helps businesses to protect data using different rule-based masking techniques such as anonymization, pseudonymization, etc. across all sensitive personal and business critical data identifiers both in production and lower environments.

Business Challenges

Organizations seek to protect data by anonymizing, deleting, or encrypting personally identifiable information in different data sources and struggle with the following –

- Lack of clarity on the fields which need to be anonymized
- Confusing pseudonymization techniques with anonymization
- Irregular application of rules across schemas
- Incompatibility with Data Quality Framework
- Unauthorized access to PII in production support
- PII data exposure in unstructured file formats like log files, emails
- Absence of single privacy console in managing, informing, and enforcing usage policies
- Lack of data traceability and data inventory
- Absence of subset copy of production data with masked PII fields in lower environments
- Lack of awareness on sensitive data fields in lower environments
- Non-compliance with global self-regulatory frameworks

How It Works

LTIMindtree Maskot can configure anonymization rules, algorithms, data inventory builder, data retention timelines, and access monitoring to assist in the following-

Data sharing across different stakeholders (internal/external) and geographies

Addressing consumer rights such as CCPA Delete, GDPR Right to be Forgotten, etc.

Data minimization

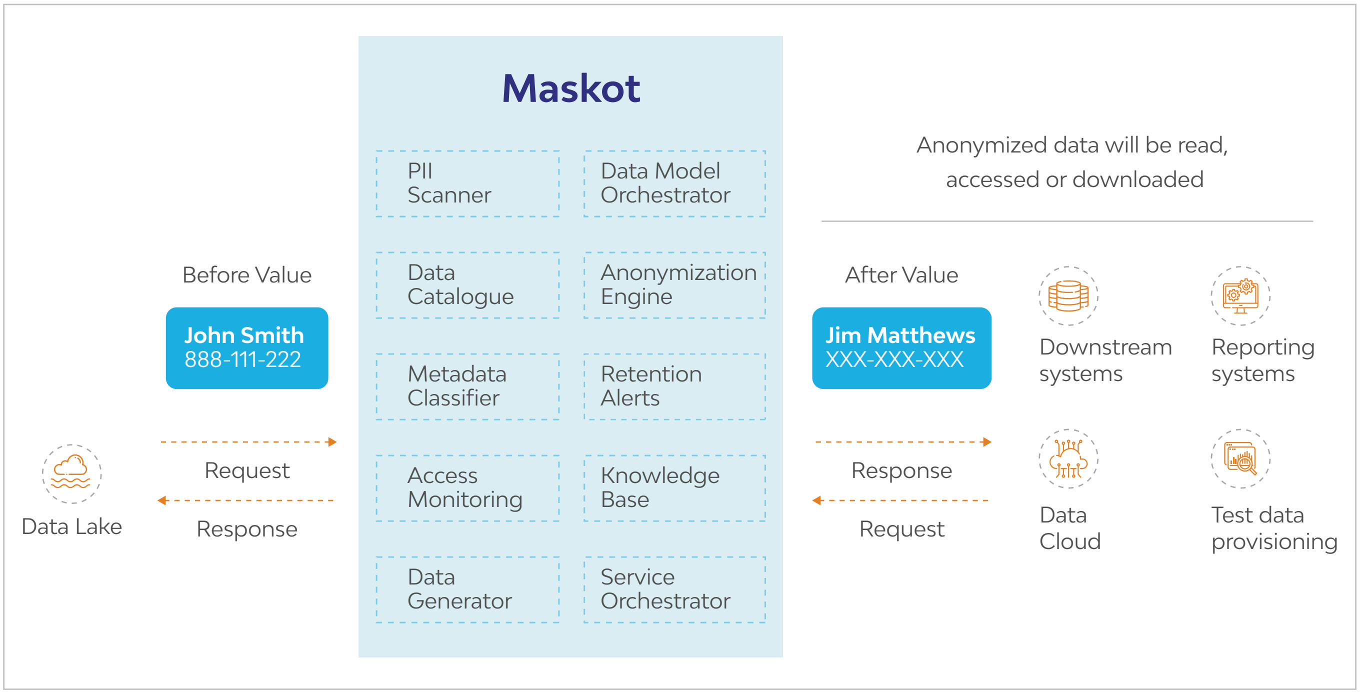
Test data management

Role & location-based masking

File labelling and object tagging to restrict the access based on defined labels, tags, and policies

Applying static data masking techniques on production database copy

LTIMindtree - MASKOT



Maskot

PII Scanner

Data Model Orchestrator

Data Catalogue

Anonymization Engine

Metadata Classifier

Retention Alerts

Access Monitoring

Knowledge Base

Data Generator

Service Orchestrator

Before Value

John Smith
888-111-222

Request

Response

Data Lake

Anonymized data will be read, accessed or downloaded

After Value

Jim Matthews
XXX-XXX-XXX

Response

Request

Downstream systems

Reporting systems

Data Cloud

Test data provisioning

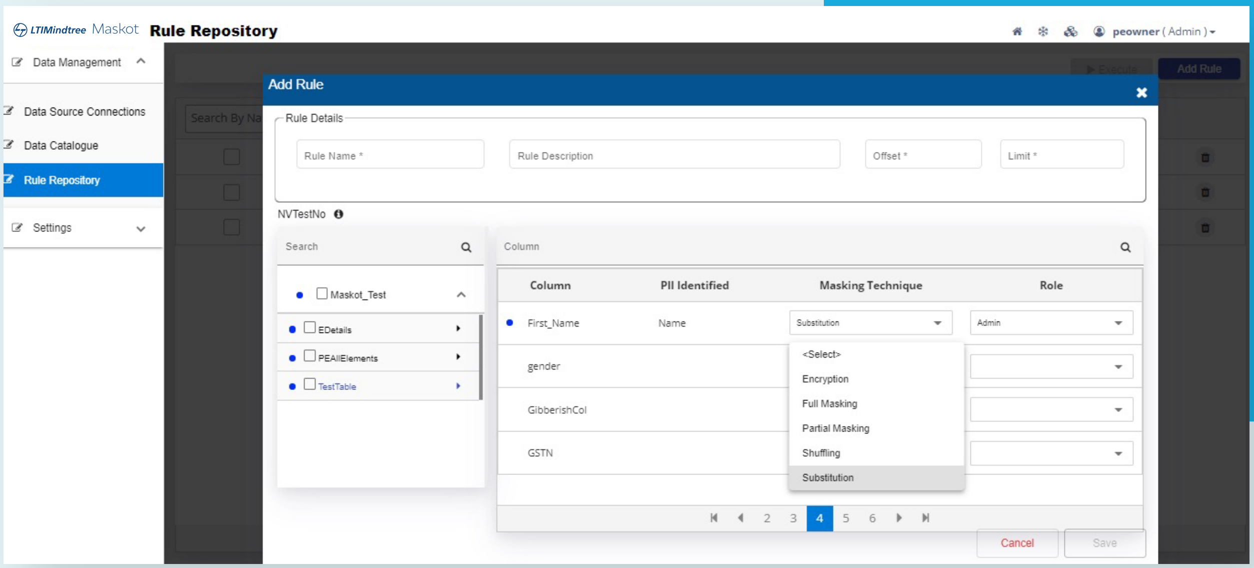
Unique Features of LTIMindtree Maskot

- Data discovery engine to create catalogue of fields to be anonymized
- Run-time anonymization and configure export to target destination
- AI-based classification to identify PII fields' lineage
- Access monitoring to track requests with PII fields
- Anonymization engine containing rules repository and protection techniques
- Automated data classification and tagging
- Retention alerts to meet regulatory guidelines
- Reporting and dashboards on anonymization and regulatory compliance
- Data model orchestrator to suggest matching data sets for test scenarios
- Data generation engine to extract or synthesize data subset
- Service orchestrator to identify data generation path, integrate with JIRA, ALM, etc., and trigger data generation engine based on configuration
- Data provisioning to lower environments by means of direct to database, insertion & creation scripts, and text files
- Role-based access control to restrict unauthorized access at file level

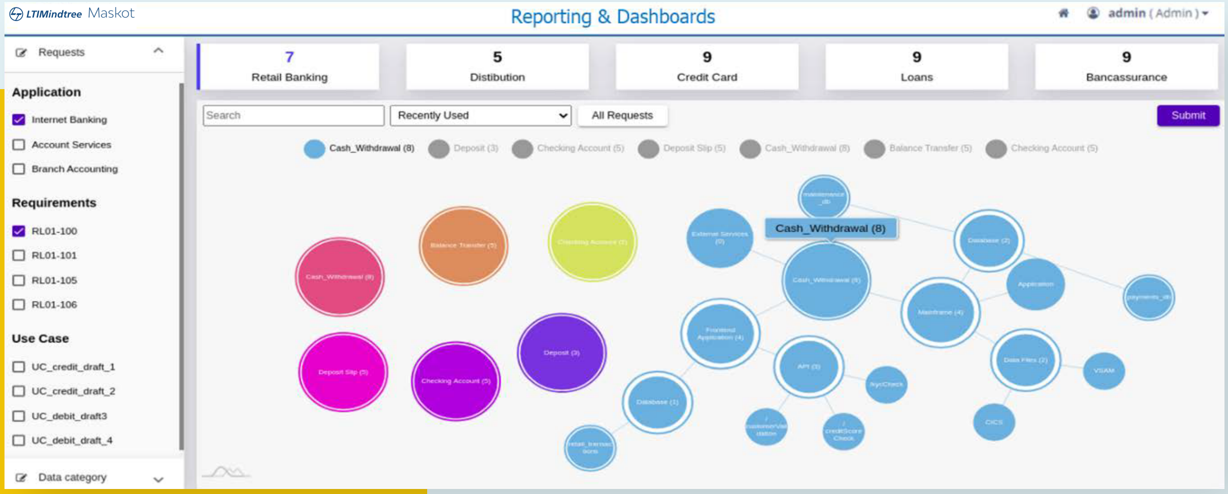
Business Benefits

- **Data profiling** to tag sensitive data fields for role-based anonymization
- **Risk minimization** as a result of secure transfers
- **Data privacy** compliance with regulations such as GDPR, CCPA, etc.
- Acts as a **Data Management Platform** (DMP) ensuring that the data is compliant for analytics across departments – HR, Sales, Marketing, Finance
- **Improved testing speed** from data reservation and synthetic test data generation
- **Automated data provisioning** sub-setting from prod to lower environments to reduce risk exposure
- **Leverage existing** privacy/security solutions viz ITSM/LDAP
- **Integrating with leading hyperscalers** and co-developing masking techniques into their cloud environment
- **Usage of static data masking** for permanent masking of sensitive information

Sneak Peek



Column	PII Identified	Masking Technique	Role
First_Name	Name	Substitution	Admin
gender			
GibberishCol			
GSTN			



LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit **https://www.ltimindtree.com/**