Securing the Cloud Hosted Applications for a Leading Retailer in Finland

Business Scenario

The customer was looking for a strategic partner to help them build and manage their Product Information Management (PIM) infrastructure on Cloud in a secure environment with better cost management while ensuring high availability and security.

Customer Challenge

The customer wanted to improve the security posture and fault tolerance of Product Information Management system that was split across various platforms. They needed industry standardized security framework and controls to secure and optimize the setup and operations of the PIM system ensuring the high availability. However, they had many challenges:

- Struggle to maintain the enormous amount of data with poor data modelling system
- Data security issues in managing database & instances
- Lack of a cybersecurity framework to secure the PIM system

The absence of solution for above outstanding challenges was impacting customer in many ways:

- Instances running at higher capacity resulted in increased operational costs and also posed availability concerns
- Absence of cybersecurity framework was exposing the sensitive data to emerging cyber threats.

Our Solution

The Product Information Management environment acts as the mainstay for any retail consumer business & Tech Mahindra was successful in helping customer to build the PIM environment on AWS enabling a fast end-to-end product onboarding and simpler asset management. On successful deployment of applications, Tech Mahindra continued to provide the Managed Services including secure provisioning, upgrading and managing the infrastructure and security operations for all environments (TST, QA and PROD). Salient features of our solution include:

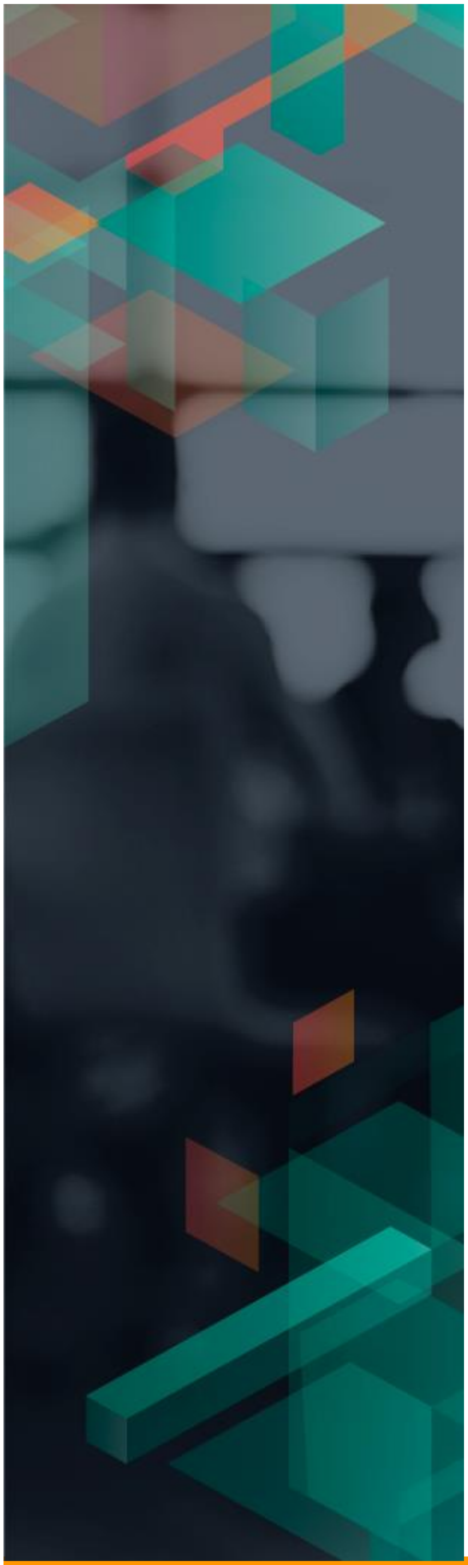
Establishing Secure framework for the cloud environment
Tech Mahindra solution backed by comprehensive and leading industry standards like cloud migration framework, Zero Trust framework, AWS well architected framework, NIST and other regulatory controls helped setup a secure by design and defense and depth model for the PIM system. By incorporating industry best and secure practices we were able to achieve optimization and create a robust environment secured from leading cyber threats.

About the Customer

A leading Retailer in Finland has business around retail, real estate and fashion brands. The company operates retail stores in European countries and online stores.

AWS Security Services Consumed:

- AWS CloudFormation
- AWS Lambda
- Amazon API Gateway
- AWS Secret Manager
- Amazon Cloud Front
- AWS Shield
- AWS WAF
- AWS IAM
- AWS Certificate Manager
- AWS KMS
- AWS Inspector
- AWS Cloud Trial
- AWS Cloud Watch



How Tech Mahindra established a robust and secure serverless architecture

The PIM infrastructure built using Infrastructure as Code (IaC) templates, which needs serverless infrastructure with lambda functions. Amazon API gateway was utilized to support it. Cloud watch and Cloud trail logging used to monitor and secure the API calls. Amazon CloudFront utilized as content delivery network (CDN) which enabled secure delivery of data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

CloudFront provided field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Amazon Route 53 to protect against OWASP application attacks including DDoS attacks.

AWS Key managed service has been utilized for data encryption and security. Policies were configured for managements, rotation and permissions on keys. AWS Certificate Manager was leveraged to secure data in transit, secure network communications and establishing identity over internet.

How Tech Mahindra established managed security services to maintain the secure posture, meeting customer’s security polices & compliance

- On completion of successful cloud transformation, Tech Mahindra continued to provide 24/7 security operations service with SOC experts monitoring the logs from cloud trail, cloud watch, compliance monitoring from AWS config and AWS inspector.
- Team also investigates alerts from AWS shield and WAF to proactively detect and mitigate cyber threats. Critical incidents are resolved on priority and reports are shared with the customers.
- Vulnerability Assessment done on AWS EC2 instances, application vulnerability assessment on PIM application to pro-actively identity high-risk security vulnerabilities and quickly remediate them on a periodic basis.
- Managing the KMS and Certificate Manager infrastructure.
- Maintaining and fine tuning the security policies on AWS Shield and WAF to improve the security posture.

Results and Benefits:

- Improved security posture - Multi-layer defense leveraging AWS cloud native security controls.
- Proactive Threat Management through Vulnerability Assessment Services.
- Integrated Security Operations and Cloud Application Management from same provider for managed services ensuring faster security incident response, quicker remediations of identified vulnerabilities and ensuring application availability.

About Tech Mahindra

Tech Mahindra’s Enterprise Security & Risk Management Services team, with 18+ years of Cyber Security experience, act as a trusted advisor – consultant, system integrator and managed security service provider. We help customers to secure their digital transformation journey by, addressing all their cloud security needs by protecting their cloud environment, providing unified visibility, and ensuring compliance.

Tech Mahindra