OpsMx + Interswitch

# *About* Interswitch

Interswitch is a leading digital payment and commerce player in Africa. Interswitch has been instrumental in transforming Africa's payment landscape by rapidly developing the financial ecosystem. Interswitch is active across the payments value chain and offers a full suite of omnichannel payment solutions.

# The Challenge: To deliver frequent innovation and provide sustainable payment solutions

Interswitch provides a network and payments platform across Africa and has been instrumental in the development of the Nigerian payments ecosystem. Interswitch has provided a full suite of Omni-channel payment solutions to critical mass in Africa, and wanted to accelerate the pace of innovation in the financial value chain. However, its software delivery process was full of challenges that impeded their pace of innovation.

## Script-based deployment was time-consuming

Interswitch migrated from traditional software to microservices and containerized applications. Initially, various teams wrote numerous scripts using Jenkins and SSH plugins to automate deployments into multiple environments. But, as the pace of innovation increased, they realized the non-standardized deployment process involved maintaining scripts that made software deployments slow and complex.

## Complying with financial regulation was challenging

Being in the finance industry, Interswitch has to strictly comply with regulations and standards. It was challenging for the IT team to manually address policy checks and adhere to SDLC regulations set by the compliance team. Moreover, it was difficult for their compliance managers to audit, and investigate non-compliance issues.

Interswitch needed a tool that could streamline the entire software delivery process, eliminate excessive dependence on tribal knowledge with respect to adherence to compliance requirements, and handle scale.

## Need for Secured Delivery

Interswitch provides all the safeguards necessary to reduce the risk of loss, unauthorized access, disclosure of personal information. They store and process personal information in their own data centers. Interswitch IT uses firewalls and data encryption mechanisms to control access to its data centers.

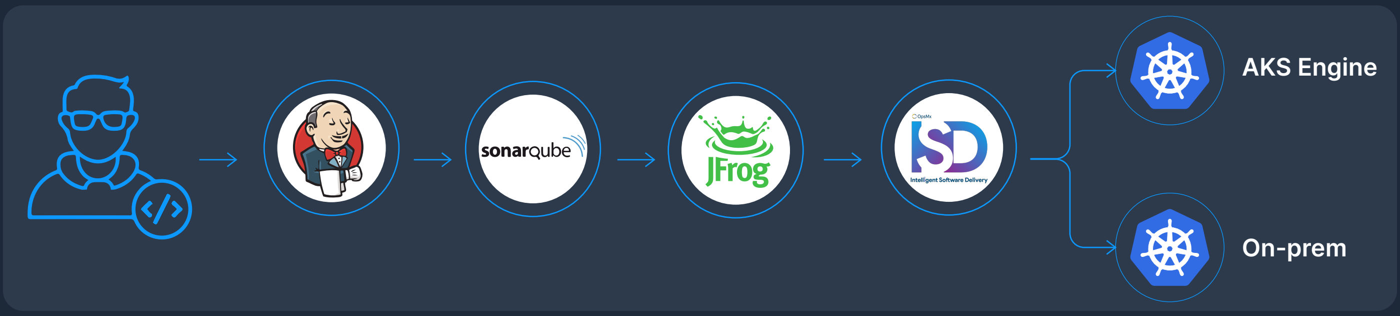
For security reasons, they have their production Kubernetes clusters configured in on-prem data centers. And there was no proper mechanism to deliver applications automatically into secured clusters.

# Solution: A scalable CD platform to speedily & safely deploy apps into Kubernetes

After evaluating a few closed-source solutions, Interswitch chose OpsMx Intelligent Software Delivery platform because it provided them the extensible and scalable orchestration layer- OpsMx Enterprise for Spinnaker, based on open-source Spinnaker, and an intelligence layer- OpsMx Autopilot, to help the IT team deploy software safely and securely.

## Automated software delivery process

Interswitch is using OpsMx ISD to automate its end-to-end software delivery pipeline by integrating with various DevOps tools such as a source code management system (BitBucket), a CI system ( Jenkins), a vulnerability scanning tool (Sonarqube), and an artifact repository (JFrog). Their DevOps engineers and developers are using ISD to securely deploy applications into Azure Kubernetes Engine (AKE) and on-prem Kubernetes behind the firewall.



## Delivering applications at scale

Nearly 100 developers, 10 DevOps engineers, and project managers use ISD to orchestrate the deployment and delivery of their payment applications. Moreover, ISD provides a standardized way to deploy into Kubernetes clusters, which was earlier done through scripts like ***Kubectl*** commands.

## Safe Release with Automated Canary Analysis

Interswitch DevOps team use ISD to perform canary analysis and estimate the risk of a new software release. ISD Autopilot gathers metrics of canary and baseline pods and applies AI/ML to perform a risk assessment. It also carries out automated decisions to roll out or roll back the OES pipeline based on the risk score.

## Compliance of SDLC process with finance regulation

Autopilot helps the DevSecOps team to address the regulatory and compliance concerns by allowing them to define policies and enforce them in OES pipelines. A few examples of policies that are used in Autopilot policy gates are:

- valid YAML in Kubernetes manifest,
- production config files must not contain UAT parameters,
- Dockerfiles must be hardened and only use a compliant base image,
- only QA can approve automated tests,
- all security scans below 80% must be manually approved,
- Blackout Window Period,
- Terraform plans by developers must not have delete action in any resource other than a VM.

With the OpsMx ISD platform, all the software must pass through automated policy gates before getting into the production environment, thus ensuring security.

> **With OpsMx, we have gone way ahead of what we could do with Spinnaker**
>
> Abdul Basit Kabir, DevOps Engineer, **Interswitch.**

## Automation of change management process

Before OpsMx Intelligent Software Delivery (ISD), the change management process was difficult as stakeholders would take days to log into the ticketing system and approve or edit a ticket with respect to pipeline execution.

Today ISD has been integrated with ServiceDesk and custom stages are built in the pipeline to create and close a ticket on successful execution of the pipeline. Approval gates are also made a part of the ISD pipeline; which means instead of manually activating it, the ISD pipeline would automatically get promoted on approvals from the right manager.

## End to End Deployment Visibility and Audit

Autopilot provides the ability to identify deployment failures in the process of software delivery with end-to-end visibility, and tracks the progress of software delivery at all times, from dev to UAT to production. Stakeholders also get an Audit report for a particular time period on any policy violations, pipeline failures, wrong deployments, etc.

# Results:

OpsMx Intelligent Software Delivery platform helped Interswitch DevOps and program managers to transform their software delivery, and the much-needed boost to accelerate their innovation with faster, frequent, and safe release processes.

## Code check-in to production times have been reduced from days to hours

The application team and DevOps team are able to deploy 100+ microservices and monoliths into production faster with ISD pipelines streamlining their deployment and delivery process. Their lead time - from code commit to production release - has now been reduced from days to hours.

> The goal of reducing deployment timelines was made possible by OpsMx Intelligent Software Delivery platform. As everything is streamlined under one umbrella, there was a 70% reduction in the lead time to move code to production
>
> says Grace Akinsola, Program Manager at **Interswitch.**

## The change management process takes hours instead of days

With ISD automatically creating, updating, and closing tickets, the dependency on manual updating of tickets and starting/halting a pipeline has been eliminated. The automated change management process now just takes hours instead of days.

## 900+ applications are automatically getting deployed using ISD

Today Interswitch IT is adopting ISD at a faster rate. To date, 100+ developers and DevOps engineers have configured 600+ pipelines to deploy 900+ applications into AKE and on-prem Kubernetes.

## Reduction of deployment risk

With ISD Autopilot verification gates, their IT team is now able to assess the risk of all the software before they are released into production.

## 100% compliant to regulation

Interswitch has eliminated the risk of policy violation with automated policy checks in their ISD pipelines.

## Lower MTTR with visibility and traceability

Interswitch reduced time to resolve issues through rapid diagnosis of issues with end-to-end visibility