

## Case Study:

# Global Fintech leader integrates mainframe into Splunk® with Ironstream

## Overview

A large financial services company had become a leading provider of core banking services that underpin credit card transaction processing for millions of consumers and businesses worldwide. Like many major corporations, the company had relied for decades on massively powerful mainframe systems to run its business.

But today, no corporation of size can compete without extensive use of modern IT operations management platforms that provide real-time, enterprise-wide visibility into what's going on across their infrastructure. The company invested in Splunk to get this single comprehensive view. However, when it wanted to extend Splunk's world-class analytics capabilities to its mainframe systems, it quickly became apparent this would be no easy task. The complexities of mainframe architecture, data formats, and programming made it all but impossible to achieve with in-house efforts. It needed to find a more workable solution.

## Business challenge

The firm's core transaction systems rely on the IBM Z platform because of its unequalled power and speed for batch and transaction processing. Real-time approvals of credit card transactions require ultra-fast processing, from ensuring available balances to confirming CVV security codes, comparing normal account behaviors, checking against fraud detection systems, and much more. And these checks must be completed within milliseconds per authorization transaction to ensure that customers and merchants are not left waiting.

In addition to such real-time services, many batch processes must be run nightly against millions of accounts. These processes generate monthly statements, calculate interest and minimum payments, create new credit cards and pins, account behavior scoring, and much more.

Mainframe performance is robust and comprehensive. But its native monitoring, alerting, and reporting can be less impressive. It tends to be on-platform, siloed, the realm of subject matter experts, and out-of-step with modern ITOM solutions such as Splunk.

## Challenge:

- Fintech leader relies on mainframes for unparalleled transaction processing power, and needs to include these critical systems in their Splunk platform for comprehensive analytics
- Complex mainframe data formats and programs don't natively integrate with Splunk, and manual efforts are unworkable

## Solution:

- Ironstream automates the collection and forwarding of critical mainframe logs, and makes the data usable in Splunk dashboards
- Provides complete, real-time visibility into mainframe machine data to perform correlation and analysis of events from across their IT infrastructure

## Benefits:

- Better, more reliable business decisions and better service for their customers
- Proactive IT operations, troubleshooting and issue resolution
- Greater return from their investments in Splunk and the mainframe
- Increased efficiency and fast time to value

## Technical Challenge

The company attempted to develop custom mainframe programs for monitoring its applications, but those efforts required many months of work. Even then, because they had to run in tandem with production transaction processing, gathering of information added significant costly CPU overhead.

Making things worse, the interface screens for these solutions only displayed results in real-time and had to be physically monitored, with eyes on the console. So, these custom applications were only run when absolutely necessary to investigate critical issues and then shut down.

Before long, the company concluded that the mainframe is extremely good at providing transaction services but not nearly as good at providing information about what is taking place right now or what may happen in the near future. In short, its mainframe systems couldn't provide the level of real-time visibility and business insights that were needed by a wider audience.

## Solution

Splunk enabled detailed reporting and management of system and application response times and throughputs and provided alerts of outages or unusual activity. It was clear that similar capabilities were needed for its mainframe systems.

Researching the problem, the company's application development and mainframe management teams soon realized that the mainframe was, in fact, generating all the systems and application processing data required to support ITOM and business analytics. The objective was to get that critical data from the mainframe to the existing Splunk solution for processing in as close to real-time as possible. In the end, the company implemented Precisely's Ironstream mainframe log forwarding solution.

Ironstream enables full integration of mainframe systems into Splunk and other leading modern platforms for enterprise-wide IT operations, service intelligence, security information, and event management.

With Ironstream, companies gain comprehensive, real-time visibility into mainframe machine data to perform powerful correlations and analyze events from across their infrastructure. These insights drive better, more reliable business decisions and faster, more accurate IT operations troubleshooting, as well as issue prevention and resolution.

Initial implementation focused on better visibility into mainframe utilization and throughput by integrating RMF and SMF records into the existing Splunk solution. Critical operating system and hardware performance data were delivered continuously to Splunk, including key information such as CPU utilization, transaction volumes, and how long batch and other processing were running. With this information, the company could quickly identify and alert on any abnormal activity levels such as CPU spikes, unusually high authorization volumes, and application outages.

Before long, the company concluded that that IBM mainframe is extremely good at doing the work of providing transaction services, but not nearly as good at providing information about what is taking place.

## Benefits

Once its initial Ironstream framework was in place, the company built out beyond system monitoring to quickly support business analytics. By creating new dashboards in Splunk, the company could gain more contextualized views into its application data. New dashboards did not require any reconfiguration in Ironstream or Splunk. Additionally, it did not require any expert mainframe administration or programming knowledge. Ironstream handled all the intricacies of identifying and delivering the relevant data to Splunk.

The result was far richer and deeper visibility into the company's most critical business processes. The company could answer such questions as - how many APIs were running for internet and mobile banking, and how customers interacted with the company - checking account balances, inquiring about a particular transaction, changing their address, etc.

With Ironstream having proven its capabilities, scalability, and ease of use, the company has begun developing even more in-depth analytics, particularly around fraud detection and customer behavior analytics.

Looking forward, the company has confidence in the Ironstream solution. The company knows Ironstream can give them real-time access to highly valuable business information previously locked up in its mainframe systems. Delivering data at a "right now" level of speed and agility ensures it will maintain its leadership in the market.