precisely

Customer Case Study:

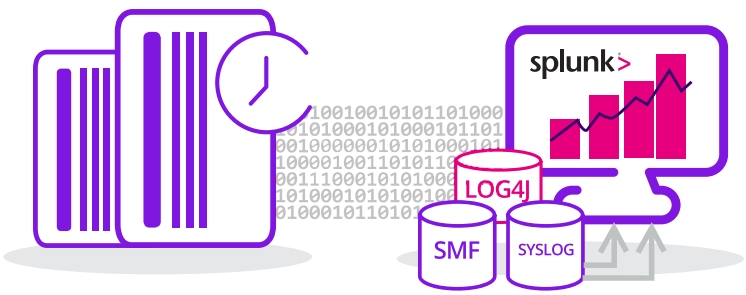
# Insurance Company Turns to Ironstream for Splunk® for Security and Compliance

## Challenge

A large North American insurance company, a national leader in automobile and home insurance, had to eliminate a significant security and compliance exposure in its z/OS environment. The problem was having only limited visibility into the status of customers' sensitive information when an application was moved across their different production and test environments.

That sensitive information was well secured in applications running on their production mainframe system. However, to guard against unnecessary exposure, as well as for compliance purposes, the data needed to be scrubbed of sensitive information when an application was sent for testing, etc., on the z/OS test system.

Fortunately the company was already using the industry-leading Splunk® Enterprise analytics platform to index and analyze operational data coming from devices in its open-systems infrastructure. But it still lacked an easy, cost-effective way to get that kind of operational data into the Splunk platform from its z/OS systems.




## Solution

The company reviewed options, focusing particularly on product compatibility with Splunk and vendor expertise in both mainframe and big data. On completing the review, they chose Precisely Ironstream to supply the missing link between its z/OS systems and the Splunk platform. Ironstream for Splunk® is the industry leading solution for collecting a variety of operational log data from IBM z/OS systems, transforming it securely into an efficient format for operational and big-data usage, and sending it to the Splunk platform — all in real-time or near real-time.

Information sources in z/OS, such as Syslog, SMF, log4j, and Unix System Services (USS) logs, are easily available for analysis and visualization, and displayable through an ordinary web browser. Also important, Ironstream eliminates the user's need for increasingly scarce z/OS expertise and costly, specialized equipment to access operational data on the mainframe.

After satisfactory completion of a Proof of Concept (POC) exercise, the company deployed Ironstream with the Splunk platform. They are now able to easily see SMF records across their various systems, to sift through the data with analytics and similar techniques, and to visualize the results in a variety of contexts, further enhancing security across their enterprise.

This insurance leader now has a clear view into all data movements across their mainframe infrastructure, ensuring that they are in full compliance with industry and corporate mandates, and ready for any audits that might arise. Ironstream enables the company to have visibility into:

- How much data is moving from one system environment to another — i.e., from production to test.
- Which protocols are being used to move data — e.g., FTP, Direct Connect, XMIT, etc.
- How, where, and who is initiating data transfers.
- Whether the inbound data to a system is coming from a production or test environment.
- Whether the data movement is compliant, non-compliant, or unknown.
- Whether approved exceptions are enabling potential unauthorized access to secure information.
- Whether data are going through the appropriate "scrubbing" as they are being moved.

In the insurance and financial services sector, enterprise-level security isn't merely desired, it is mandated by regulation and required for customer trust. Using Ironstream for Splunk, this leader in the insurance industry was able efficiently and seamlessly to address its security and compliance concerns.

**To learn more about this solution, visit: www.precisely.com**