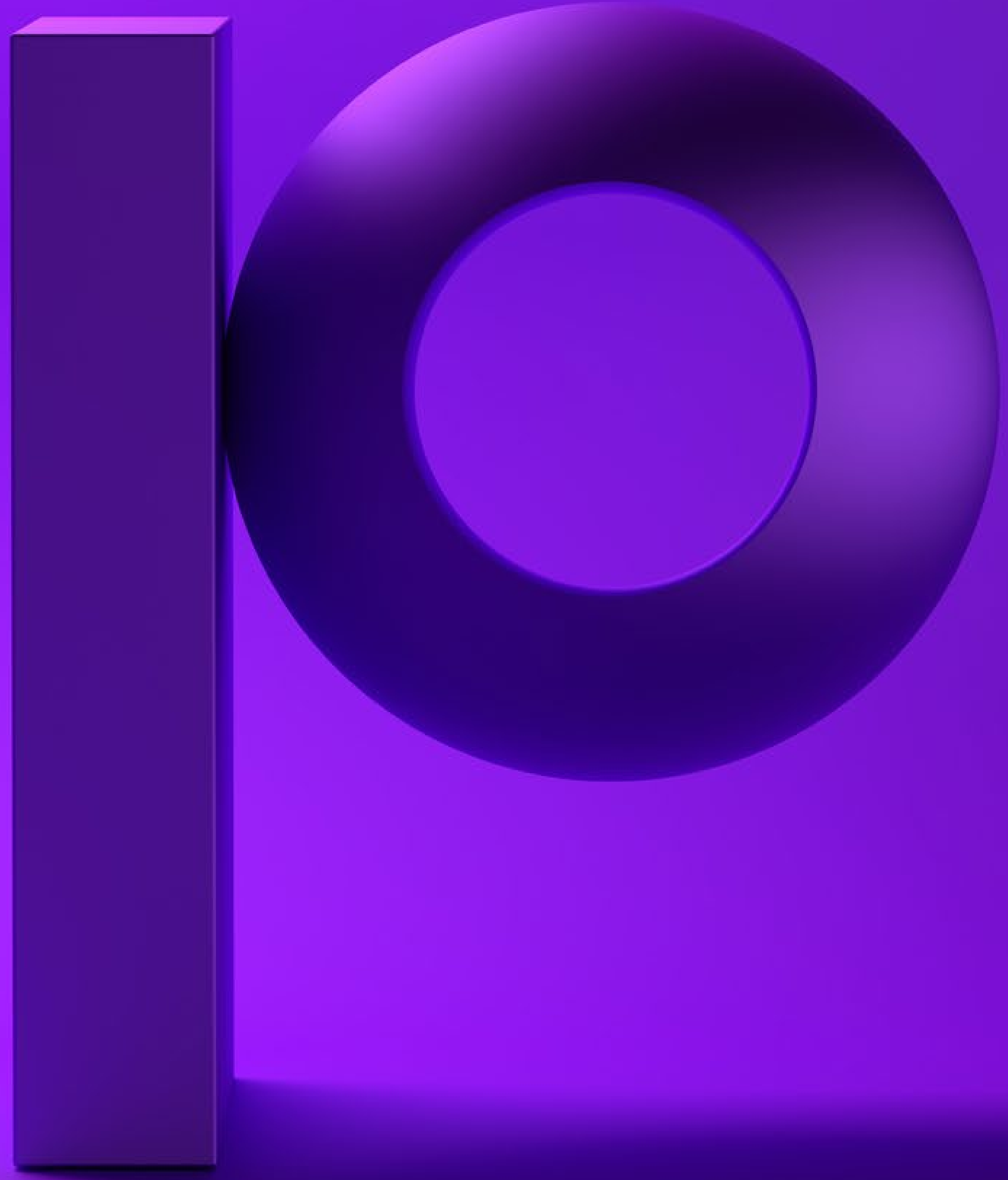
precisely

# Splunk and the Mainframe:

## 6 Real-World Case Studies for ITOA, ITSI and SIEM



# Primary Use Cases

There are a number of different data sources that are available within the IBM z/OS mainframe that can be leveraged to provide insight into the operational health of the system and applications as well as providing visibility into security and compliance issues. For example, the System Management Facility (SMF) on z/OS collects and records a large amount of information on performance, security, and technical operations. Terabytes of very useful information can be recorded daily. Virtually every operational event that occurs on the mainframe — from a simple log-in attempt at a particular workstation to a potential breach of system security — is captured and recorded in one or more SMF record types.

The challenge has been how to easily extract and analyze this data to answer the questions that need to be answered.

Today most organizations are still challenged to answer questions like: What is the health of my IT infrastructure? How well are my applications performing? What problems are impacting availability? When do I need to plan for additional capacity? Are we meeting our established Service Level Agreements (SLAs)? Are our IT services meeting the expectations of our customers and end-users? Are we exposed to potential security threats? Can we produce the necessary audit trails and reports required to meet compliance initiatives?

The answer to these questions are typically addressed through the process of analyzing, managing, and recognizing the patterns and anomalies available within IT operational data. There are three specific use cases which have emerged to encompass these analytical processes.

## IT Operational Analytics (ITOA):

An approach to IT operational data that allows for better understanding and enabling better decisions about managing the IT environment. ITOA typically applies Big Data principles to the IT environment providing a broader context—and clearer operational intelligence—about what's happening.

This bigger picture of what's happening in the environment enables organizations to make better decisions to take control of the IT infrastructure and ensure that they are achieving operational efficiency.

## IT Service Intelligence (ITSI):

Delivers a central, unified view of critical IT services for powerful, data-driven monitoring by mapping critical services with Key Performance Indicators (KPIs) to easily pinpoint what matters most. ITSI provides business and service context to prioritize incident investigation and triage with support for drill downs to profile an entity and rapidly troubleshoot outages and service degradations. Some ITSI implementations will use machine learning to detect patterns, dynamically adapt thresholds, highlight anomalies and pinpoint areas of impact.

## Security Information and Event Management (SIEM):

Technology that aggregates and provides real-time analysis of security alerts using event data produced by security devices, network infrastructures, systems and applications. A primary function of SIEM is to analyze security event data in real time for internal and external threat detection to prevent potential hacks and data loss.

This typically includes user behavior analytics (UBA) – understanding user behavior and how it might impact security. SIEM technologies also collect, store, analyze and report on data needed for regulator y compliance to ensure that audit requirements are met as dictated.

# Major Insurer Achieves IT Operational Efficiency with ITOA Solution

## Mainframe IT and business IT both get big data benefits

**Challenge:** Organizations constantly look to extract more value from the operational data generated within their IT infrastructure, and to analyze that information to determine how their systems and applications are performing.

A primary source of operational intelligence for IBM z/OS mainframe users lies in the SMF (System Management Facility) records.

These are recorded for just about ever y event and activity on the system. In order to extract such valuable information, organizations typically are saddled with the time-consuming manual processes of offloading the data, extracting the relevant records and fields, and then transforming the remaining subset with expensive tools like SAS.

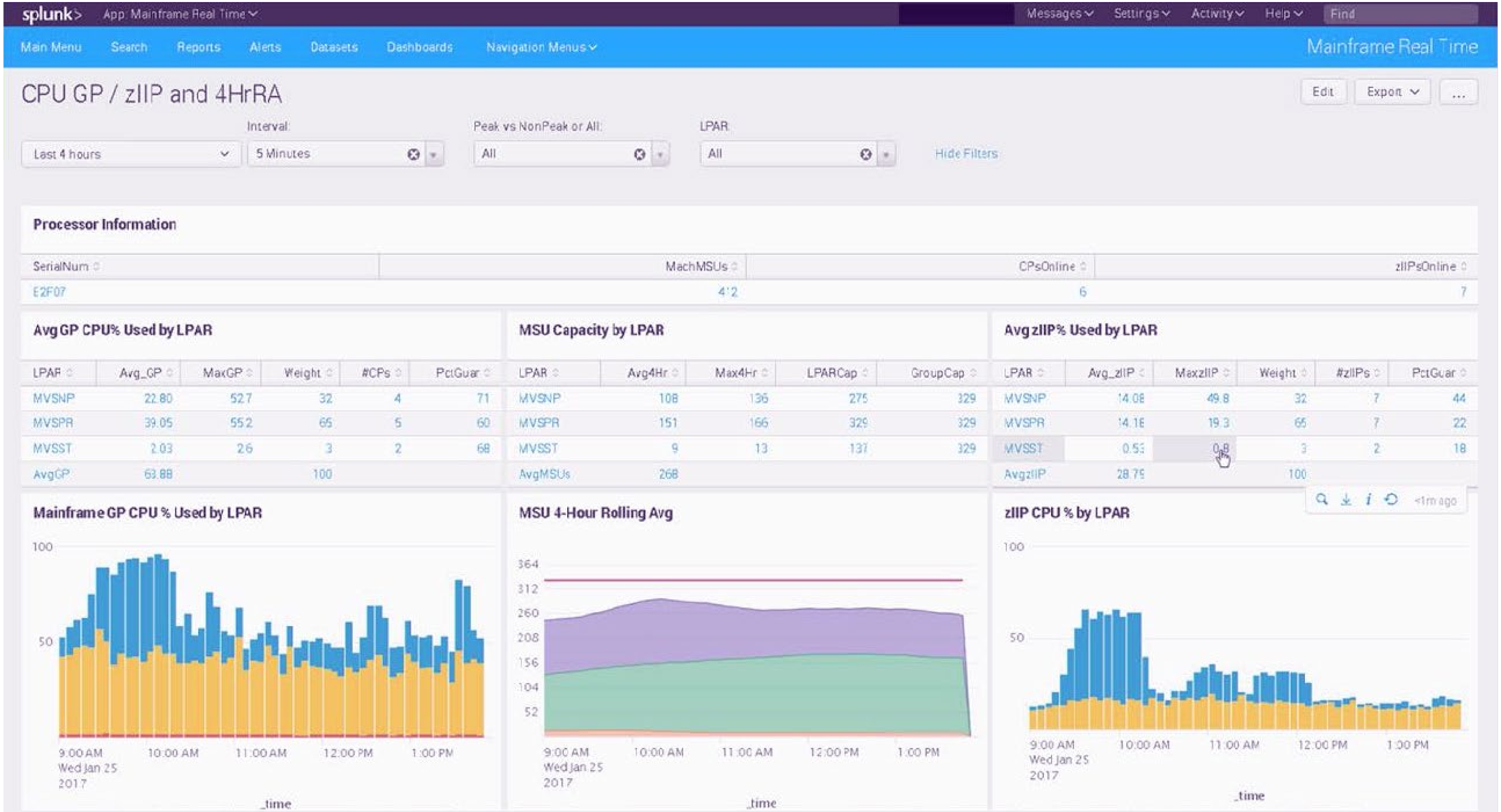
These are often multiple-day processes that fail to answer certain essential questions, such as: What is happening now? Is what is happening now different than what was happening this same time last week or the same time one month ago? Can I predict or even prevent issues from impacting performance or adherence to service level agreements (SLAs)?

This process is then repeated across the multiple LPARs that exist in most organizations, making it even more time-consuming and increasingly difficult to get complete visibility across the enterprise.

**Solution:** One major insurance company had been dealing with this challenge in the same way as most other organizations. They were offloading SMF data daily, extracting the required records and fields, then doing post processing using SAS to generate reports on the desired information. As a possible alternative, however, they were intrigued by the concept of ITOA (IT operations analytics), by which their own data could be empowered to let them better understand and ultimately to improve their operations. And so they researched the leading ITOA vendors.

They then began to use Splunk® Enterprise for analytics and visualization of critical IT components. But they were still relying on those antiquated, labor-intensive processes to get z/OS SMF data loaded into Splunk Enterprise.

Discussing the problem with Precisely, and seeing a demonstration of Ironstream, they quickly realized that Ironstream would enable them to process and forward SMF data to the Splunk Enterprise analytics platform in real-time, eliminating the manual process.



CPU GP / zIIP and 4HrRA

Last 4 hours

Interval: 5 Minutes

Peak vs NonPeak or All: All

LPAR: All

Processor Information

| SerialNum | MachMSUs | CPsOnline | zIIPsOnline |
|---|---|---|---|
| E2F07 | 412 | 6 | 7 |

Avg GP CPU% Used by LPAR

| LPAR | Avg_GP | MaxGP | Weight | #CPs | PctGuar |
|---|---|---|---|---|---|
| MVSNP | 22.80 | 52.7 | 32 | 4 | 71 |
| MVSPR | 39.05 | 55.2 | 65 | 5 | 60 |
| MVSST | 2.03 | 2.6 | 3 | 2 | 68 |
| AvgGP | 63.88 | | 100 | | |

MSU Capacity by LPAR

| LPAR | Avg4Hr | Max4Hr | LPARCap | GroupCap |
|---|---|---|---|---|
| MVSNP | 108 | 136 | 275 | 329 |
| MVSPR | 151 | 166 | 329 | 329 |
| MVSST | 9 | 13 | 137 | 329 |
| AvgMSUs | 268 | | | |

Avg zIIP% Used by LPAR

| LPAR | Avg_zIIP | MaxzIIP | Weight | #zIIPs | PctGuar |
|---|---|---|---|---|---|
| MVSNP | 14.08 | 49.8 | 32 | 7 | 44 |
| MVSPR | 14.16 | 19.3 | 65 | 7 | 22 |
| MVSST | 0.53 | 0.8 | 3 | 2 | 18 |
| AvgzIIP | 28.79 | | 100 | | |

Mainframe GP CPU % Used by LPAR

MSU 4-Hour Rolling Avg

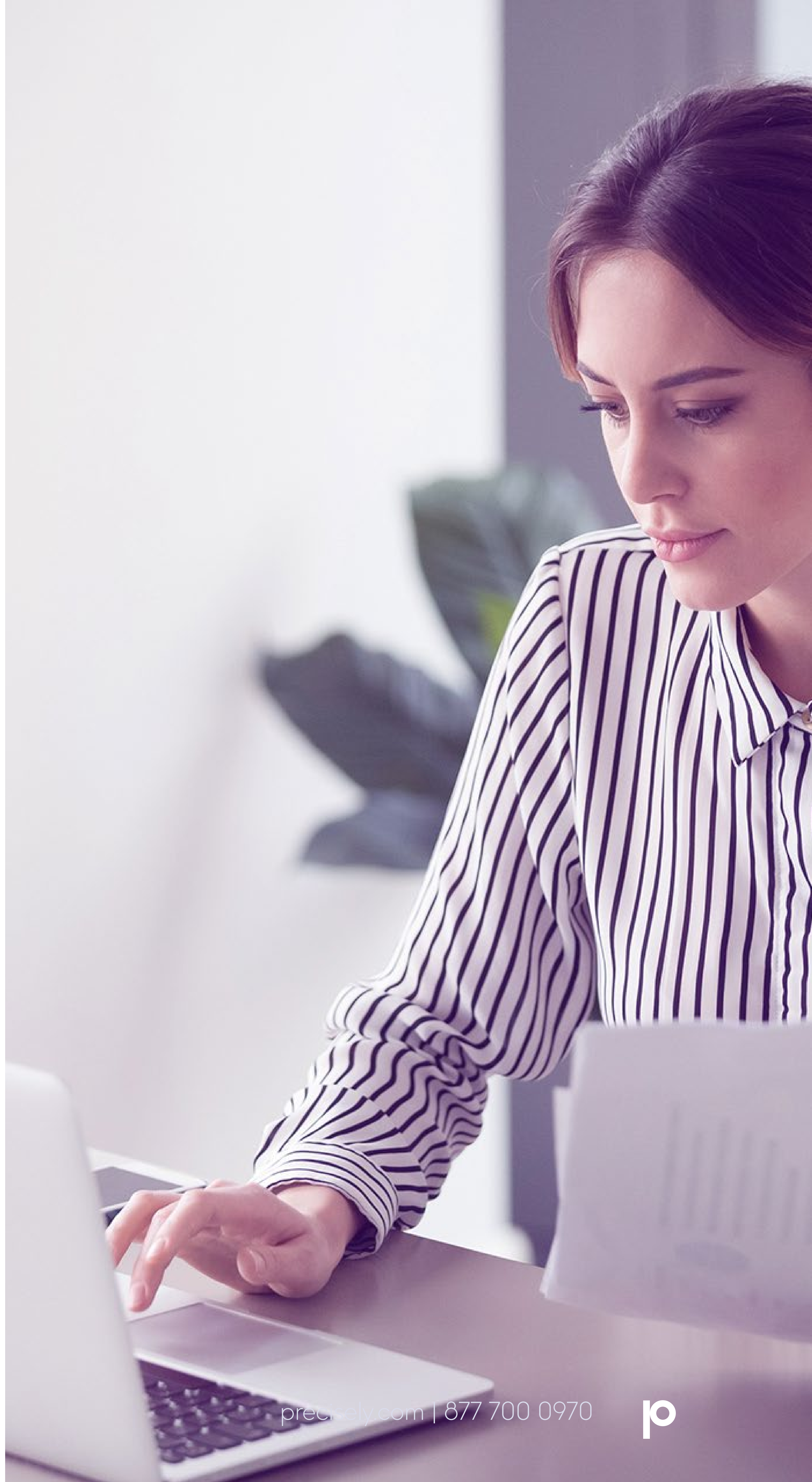
zIIP CPU % by LPAR

# Major Insurer Achieves IT Operational Efficiency with ITOA Solution

**Results:** With Ironstream in place, the customer quickly expanded Splunk dashboard development to leverage the abundance of forwarded SMF and RMF data. They implemented a full range of operational analytics across their z/OS infrastructure, which gave them the ability to measure CPU utilization across general processors and zIIP engines, and to measure MSUs (Million Service Units) against the 4-hour rolling average window. All this ensured that they were not in danger of exceeding licensed capacity and incurring additional license charges.

Some of the benefits they are able to realize using the Ironstream App for Splunk Enterprise include:

- Elimination of time- and resource-consuming manual processes for extracting and transforming SMF data.
- Historical trending of data forwarded by Ironstream to Splunk Enterprise to provide a real-time view of what is happening now and how it compares to previous points in time.
- Correlation of MQ messages with CICS, showing transaction flows for critical services.
- Enterprise-wide view of resource utilization for all z/OS LPARs correlated into a single dashboard providing visibility beyond any thing provided by existing legacy tools.
- Ability to monitor CPU utilization for general processors, zIIP utilization, and the 4-hour MSU rolling average versus defined capacity for all LPARs and combine that into a single Splunk dashboard.



# Global Financial Firm Controls Costs on IT Operations with ITOA Solution

## Enabled by real-time log analytics

**Challenge:** Banks and financial services firms have many unique challenges in this digital-mobile-global era, and choosing which to address first is an important skill for their IT leaders. Better control over a multiplicity of costly IT operations was the goal of this multinational financial services corporation. One job, for example, was using 30% more CPU time than was normal; the cause was unclear, and the impact was unacceptable.

The lack of understanding exactly "why" certain things cost so much and took so long to resolve had to be addressed to ensure they remained a leader in this hyper-competitive sector.

More broadly, the customer was spending too much money on additional capacity on demand; the mean time to problem resolution was too long; timely alerts to many problems were lacking; and there was insufficient correlation of significant events picked up by operational and application performance monitors in various business segments. Even more critically, there was no correlation between its IBM z/OS mainframes and distributed systems.

IT operations analytics (ITOA) was the primary use case the company wanted addressed, and that included several capabilities to address their business needs:

- Getting real-time alerts from RMF III and Db2 database access threads.
- Proactively monitoring statistical anomalies relating to mainframe resource consumption.
- Real-time tracking of transaction performance as transaction data moved through multiple stages from distributed to mainframe systems.
- Real-time alerting on mainframe usage and contention issues in batch job performance.
- Real-time monitoring of Db2 Stored procedures for excessive calls.
- Identifying key areas for automation or consolidation.

**The Solution:** This began with researching the IT operations analytics (ITOA) marketplace and choosing the clear leader in this big data analytics platform sector serving the high-transaction financial services firms. The customer's overall platform selection for IT monitoring and analytics, which brings together inputs from its distributed computing environment, was Splunk Enterprise. This platform was ingesting 40 terabytes of log data per day from hundreds of applications around the world.

Missing from this insight-generating stream, however, was real time performance log data, or "machine" data, from the mainframe environment. That changed when it began a pilot program for Ironstream, the chosen partner of Splunk for solutions that access mainframe log data in real time. Ironstream is the industry's premier real time forwarder of critical SMF records and other z/OS operations and applications log data to the Splunk platform. Given its unmatched track record of success in this area, Ironstream was an easy choice.

The pilot was a success, so in 2016 the customer began working toward full implementation. It involved the mainframe and Splunk savvy Precisely services team and the customer's IT team working together on a detailed business requirements roadmap, customized use case designs, installation planning, and rollout of the Ironstream + Splunk Enterprise solution across the critical operations.

By early 2017, the customer had the capacity via Ironstream to forward in real time up to 100 GB of z/OS log data from 13 LPARs to the Splunk platform. That enabled correlation and analysis with like log data from distributed systems and supported the desired new insights and efficiencies.

It was also just the beginning. The customer planned to bring on other mainframe data sources to provide additional value to the various users, with capacity expansion up to 2 TB per day anticipated. The more mainframe data accessed, the more value delivered for each additional use case.

**Performance Results:**
Once in production, the Ironstream + Splunk Enterprise solution was delivering actionable insights, including:

- Real-time CPU monitoring in Splunk Enterprise to pinpoint expensive transactions, business volumes, and other variables that correlate with MIPs usage.
- Tracking of overnight batch progress in real time, including predictive analysis to identify potential bottlenecks, to alert when SL As or other targets might be missed.
- Highlighting of key CPU consumption anomalies, with alerts.
- Tracking of Db2 stored procedures, with exceptions for lock contention and escalation, timeouts, deadlocks, excessive calls, and package wait time.
- Real time reporting, visualization, and monitoring of mainframe
- SMF data to monitor system health and identify real or potential failures in Splunk Enterprise.
- Clear visibility into mainframe and distributed-to-mainframe operations and applications in Splunk Enterprise.

**Business Results:**
- Costly CPU consumption was reduced.
- The expensive CPU processing of SAS/MXG reporting was offloaded to inexpensive commodity hardware via the Splunk platform.
- Service quality was enhanced by more effective problem resolution and reduction in mean time to resolution (MTTR).
- In-house tools made obsolete by monitoring in Splunk.
- Enterprise were targeted for elimination.
- Production of a wide range of business reports from one unified system in real time was made possible.
- Operational efficiencies and predictive analytics were driving the desired resource savings and a competitive advantage.

# Luxury Auto Network Opts for IT Service Intelligence to Improve Business Performance

## Splunk® IT Service Intelligence + Ironstream drives excellence

Business application performance that ensures that customer service operations deliver the value that the most discriminating luxury car buyer expects — that was the challenge that this Americas arm for a luxury European auto maker was striving to meet and overcome. Besides the company's own IT systems, it must also effectively support continual interactions with the disparate IT systems at several hundred associated dealerships nationwide.

For a time, however, the company 's IT staff was often becoming aware of application problems only after a dealership complained directly to the CIO. (Not good.) The thing that was missing was real time monitoring of key performance indicators (KPIs), especially for its CICS and Db2 apps.

In IT industry parlance, what this challenge called for was an IT service intelligence solution, and the premier industry solution is offered by Splunk Inc. with its revolutionary Splunk IT Service Intelligence™ premium app. So far, so good — at least as far as the various distributed systems were concerned.

Obviously, however, the vitally important CICS and Db2 mainframe performance logs were not part of the distributed systems. They were secured in "the glass house" — the company 's z/OS mainframe environment. That inner sanctum of enterprise data is normally not easily or cost-effectively accessible from the distributed environment. For this company, getting those mainframe data feeds into the Splunk platform in real time for service-centric diagnostics was crucial.

The company demands the best for both its customers and its dealership networks worldwide. It rightfully expects IT to drive value and competitive advantage — not be the source of issues from that dealer network. They want service to be 100% focused on selling and delivering a world-class experience.

**Solution:** For the Splunk sales team, the question of how to get CICS and Db2 log data into Splunk IT Service Intelligence was no question at all. It had to be Ironstream along with the Ironstream Module for Splunk IT Service Intelligence.

Precisely is a Splunk Technolog y Alliance Partner since 2014, and its Ironstream offering is the industry's premier mainframe log data access solution, which for years now has been securely streaming mainframe logs into the Splunk platform for Splunk customers. Thus, Ironstream in conjunction with the Splunk IT Service Intelligence application became this customer's solution.

**Results:** Splunk IT Service Intelligence using Ironstream as the SMF data forwarder has enabled the customer to:

- Reduce MTTR (mean-time-to-resolution) of CICS, Db2, and other production issues.
- Attain end-to-end visibility into application health and performance.
- Improve satisfaction among the dealerships in getting timely business information from the distributor.

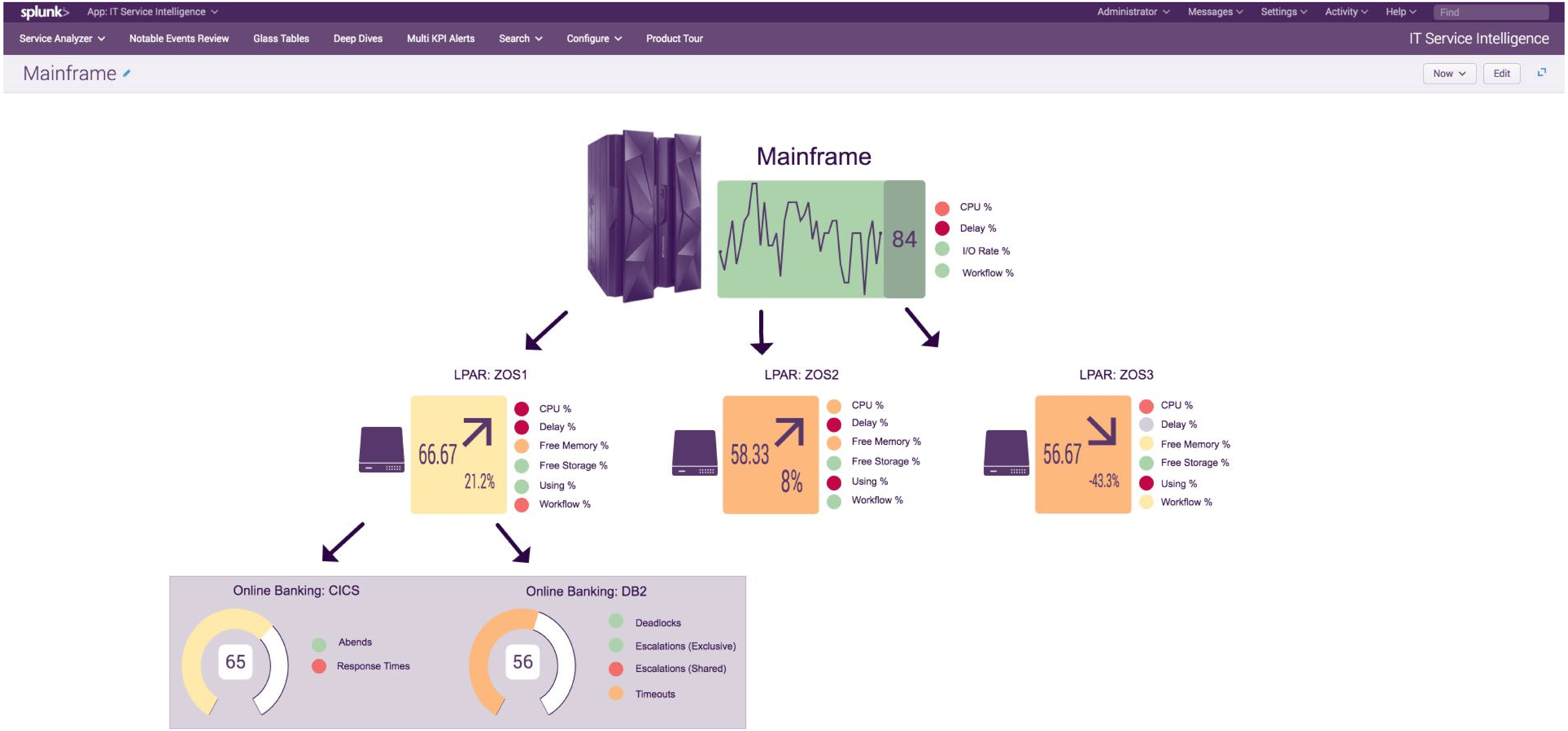


*Figure 3: An example of the kind of clickable, end-to-end "glass table"view of an entire business process now possible*

# Insurance Firm is Proactive in Enterprise Security

## Splunk® IT Service Intelligence + Ironstream drives excellence

**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 in having only limited visibility into the status of customers' sensitive personal information when an application was moved across their different production and test environments.

That personal 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 the sensitive personal 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 data-integration 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 Ironstream, a data-gathering solution developed by Precisely to supply the missing link between its z/OS systems and the Splunk platform.

Ironstream is the industr y leading platform that collects a variety of operational log data from IBM z/OS systems, transforms it securely into an efficient format for operational and big-data usage, and sends it to the Splunk platform — all in real time or near real time.

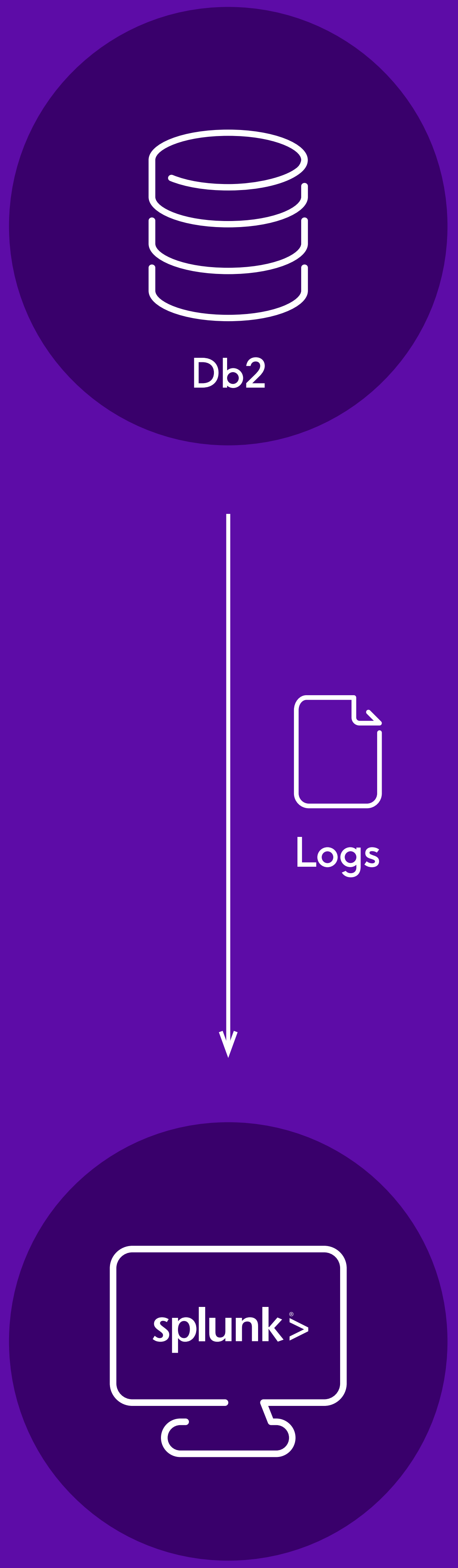
Information sources in z/OS, such as Syslog, SMF, log4j, and Unix System Services (USS) logs, are easily available for analysis and visualization, and displayable through an ordinary web browser. Also important, Ironstream eliminates the user's need for increasingly scarce z/OS expertise and costly, 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. With that, the company became able to gather the required data movement information from 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 in conjunction with Splunk Enterprise 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., F TP, Direct Connect, XMIT, etc.
- How, where, and who are 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 the 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 Splunk Enterprise + Ironstream, this leader in the insurance industry was able to efficiently and seamlessly address its security and compliance concerns.



# Agency Meets Audit/Information Security Needs

## Ironstream + Splunk help federal law enforcement

**Challenge:** A federal law-enforcement agency faced a big challenge. It had to respond to ever-changing reporting requests from its auditors in order to prove compliance with information security requirements.

For that it would need to collect and analyze operational log data from all of its many IT systems.

That intelligence would have to encompass the history as well as the current status of enterprise security information. The agency had previously chosen Splunk Enterprise as its log management and analytics platform, so it already had the ability to acquire the necessary log data from its distributed, multi-vendor, open-source environment.

But an important source of log data was still missing. That source was (and is) the agency's mainframe systems, which possessed extremely sensitive authentication information, as well as enterprise-wide details on password changes, log-in successes and failures, and accounts being locked out of the mainframe systems. All of that detail, however, was beyond the reach of Splunk.

**Solution:** An extensive search brought up one product that offered the best solution — Ironstream from Precisely.

Ironstream was created specifically for the purpose of collecting log data from the System Management Facility of IBM z/OS, transforming it to generic machine language, and forwarding it in real time to the Splunk platform.

That was all the federal group needed to know, and they moved quickly to adapt.

**Results:** The customer for the first time now has full visibility, in real time, into the most sensitive authentication procedures and data across their IT environment. They now have enterprise-wide visibility into:

- Failed authentication attempts.
- Attempts at accessing resources that are denied by the access control mechanism.
- Privileged user actions.
- Activities that require privilege.
- All attempted accesses of security-related resources, whether successful or not.
- Creation or deletion of users.
- Changes to user security information or access rights.
- Changes to system security configuration.
- Changes to system software.
- Attempts at escalation of privileges.
- All log-in activity.
- Password changes.

The agency is now able to audit for unusual activity at the individual user levels, helping them detect security exposures such as:

- Access from an unusual location, unusual network zone, or unusual time of day.
- Changes to user privileges and rights.
- Excessive data transmissions.
- Unusual movement of data.

Ironstream is an important step forward in the data-integration marketplace. It collects z/OS log data from IBM mainframes, transforms it to generic machine language, and forwards it securely to Splunk® Enterprise, Splunk Enterprise Security, or Splunk Cloud™.

That way, mainframe log data can be merged on the Splunk platform with all other machine data from distributed systems across the enterprise. Users are thus able to have a true 360-degree view of the entire enterprise IT infrastructure. Companies that use Splunk platforms can see what this may mean for them by asking the Precisely rep for the free Ironstream Starter Edition.

# Compliance Rules Lead Client-focused Co. to Ironstream + Splunk

## SOC2 certification handled by healthcare leader

**Challenge:** Organizations' mandates to get certified for the adequacy of their IT controls for regulator y compliance are a significant driver of a shift taking place in IT infrastructures. For leading enterprises, this shift includes efficiently adopting "Big Iron to Big Data" strategies, such that security and compliance-relevant mainframe data (in this case, specified SMF files) are streamed to the big data analytics platform chosen for enterprise security and compliance.

Such certification is needed so that organizations can assure their clients and customers that their sensitive information is protected. Organizations also need to "pass the audit," and for all of that they need to combine and correlate the relevant mainframe data with its relevant distributed data counterpart.

Like so many other enterprises, one particular healthcare company was having trouble meeting all the varied requirements for certification under the standard known as SOC2. The SOC2 standard focuses on non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy, and of course they apply to the systems that touch the data.

To process all the relevant SMF security records generated each day by its three IBM mainframes, this company was using IBM's zSecure products plus some home-grown elements. But that had proved to be excessively labor intensive and kept them from meeting all the SOC2 reporting requirements, especially those for the claims-processing application running on the mainframes. They needed a better solution to address the requirement and more fully address the need. SOC2 reporting requirements include the proper monitoring of log-on attempts, password changes, and user access violations. Given this system's size and growth — it manages a portfolio of diverse health-related businesses serving 50 million people — that's a lot of SMF records to access and analyze.

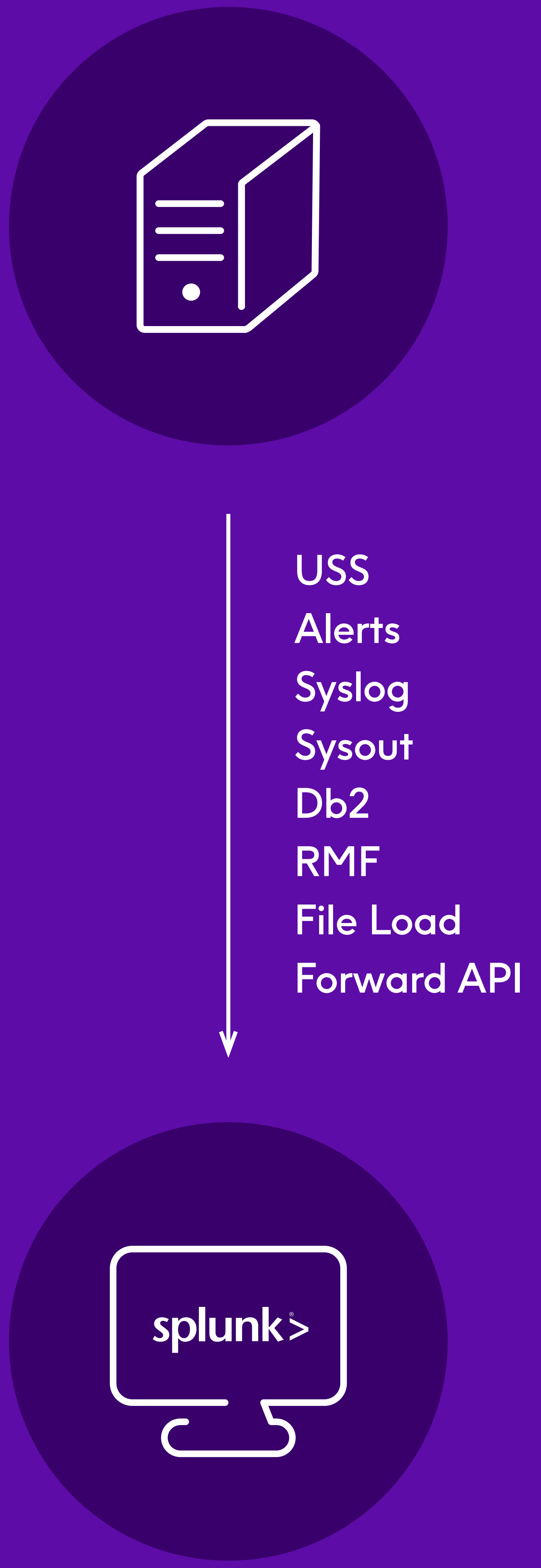
**Solution:** For some time, the company had been discussing the problem with Precisely as well as a number of other vendors in the SIEM (security information and event management) space. Their search for a solution kicked into high gear in early 2016 when they were facing important compliance targets that had to be met later in the year. Precisely quickly arranged a proof-of-concept (POC) demonstration of its Ironstream product together with Splunk® Enterprise, using a sample of the customer's own SMF data.

The POC proved Ironstream's ability to replace the zSecure manual processes. That, plus the value-pricing and the track record of the Ironstream + Splunk Enterprise combination at other companies within the healthcare industry, persuaded the company to choose Ironstream + Splunk Enterprise over the competition.

The customer began securely forwarding ~20 gigabytes of SMF records per day through Ironstream to the Splunk platform for efficient, real-time monitoring and analysis, a volume that could eventually grow to 800 GB per day when you factor in growth and having other mainframe data sources brought in. With Ironstream's innovative filtering, though, they can minimize the streamed data to include only those that are relevant to the use case.

### Among the Results:

- The monitoring of security activity on their mainframe applications in Splunk Enterprise, including log-on attempts, password changes, user access violations, etc., met the audit and compliance thresholds for SOC2 certification.
- The manual processes and related efforts and costs associated with using zSecure were eliminated.
- The SMF forwarding became automated and started being done in real-time.
- They were able to select and forward to Splunk Enterprise only those records related to security and compliance, without having to process the entire SMF record set, significantly reducing the volume of data forwarded and controlling resource consumption. With Ironstream's industry-best file-type support, low overhead, and innovative filtering, this healthcare leader can easily expand to other use cases while keeping costs to a minimum. They are equipped to garner new insights from their data and can easily adapt to changing needs.

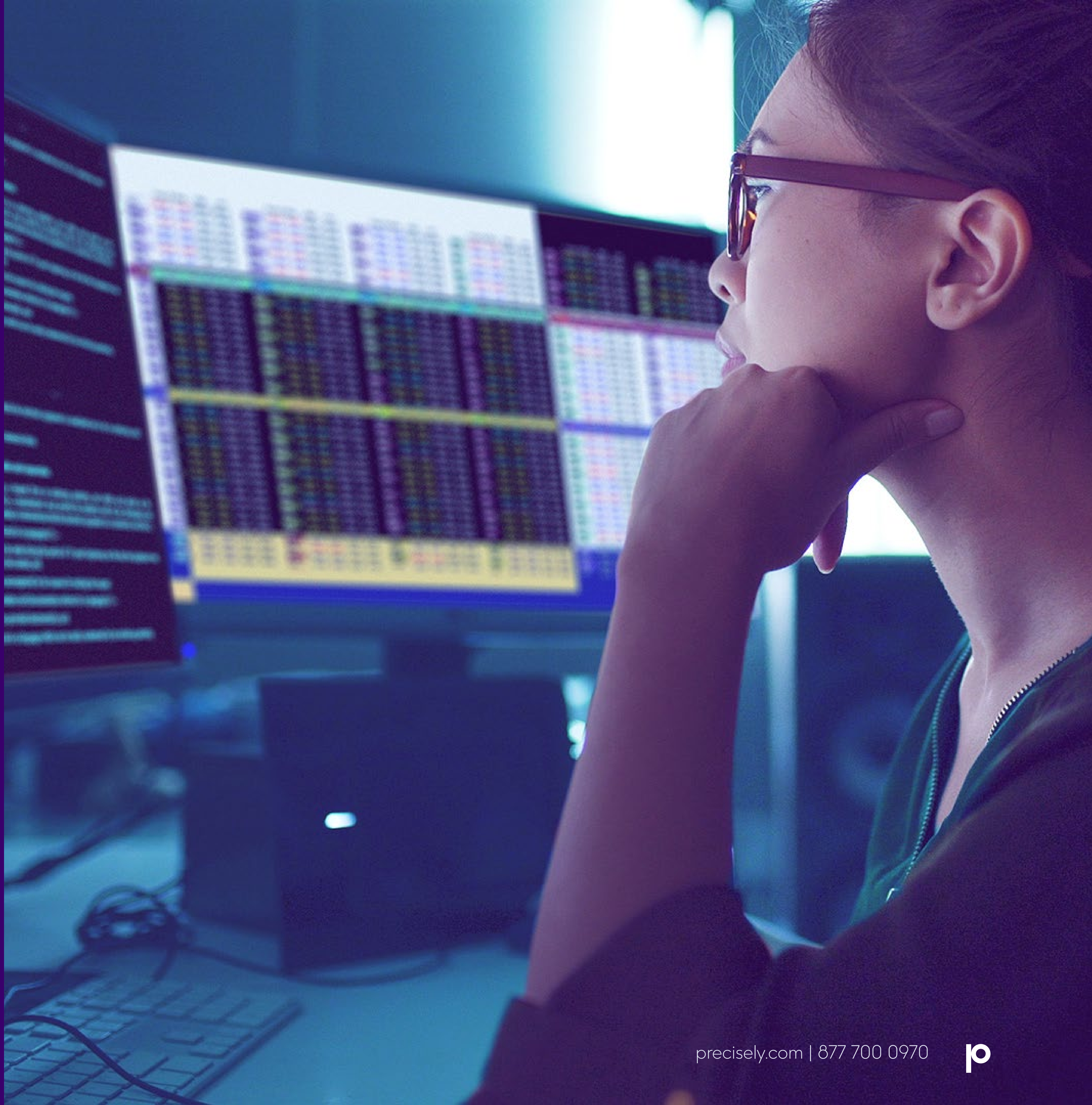


# Conclusion

Ironstream running with Splunk represents an easy, cost-efficient way for an organization to get answers to the questions centered around operational excellence, IT service intelligence, and security & compliance by integrating critical information sources, key performance indicators and events contained across the different logging facilities within the z/OS operating system.

Organizations across all vertical industries including banking, financial services, insurance companies, manufacturing, and government agencies are leveraging Ironstream to help them:

- Achieve higher operational efficiency
- Perform better problem-resolution management
- Ensure healthier IT operations
- Map critical services with KPIs of related IT components
- Easily pinpoint where problems are impacting service delivery
- Get clearer, more precise security information and alerts
- Identify potential security threats and risks in z/OS
- Address audit mandates and meet compliance initiatives



precisely

## About Precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely's data integration, data quality, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

**www.precisely.com**