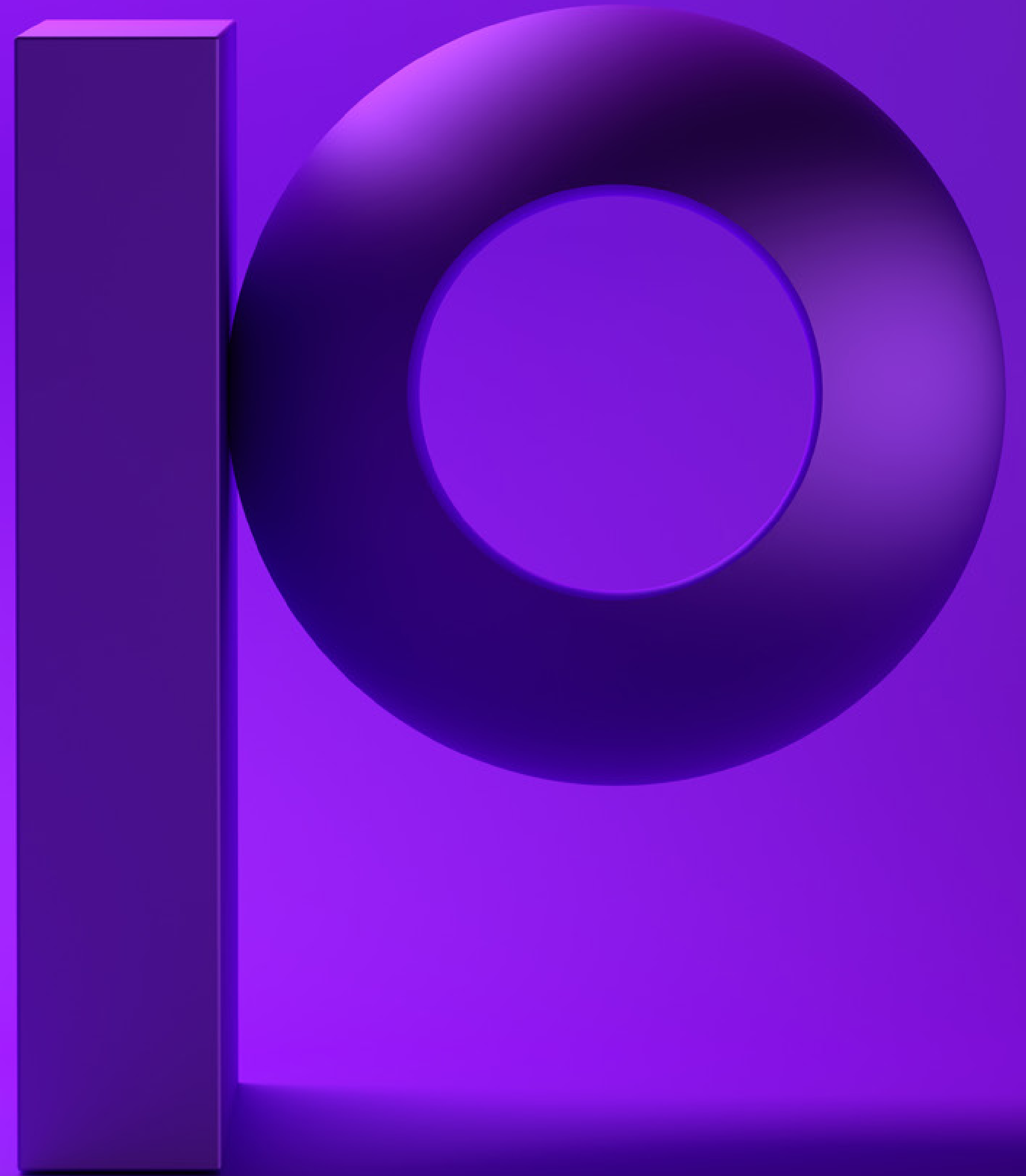


precisely

# IT Operations Checklist for z/OS Mainframes



# Introduction

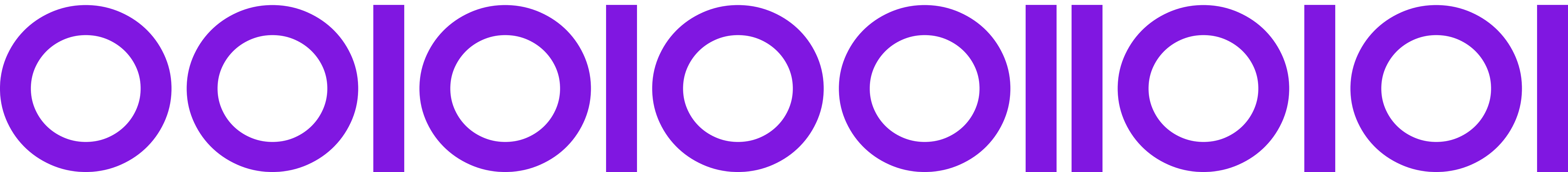
For the past several decades, monitoring the overall health of IT components running on IBM's z/OS mainframe has been left to a number of vendors specializing in real-time monitoring of performance and availability. Although they have done a more than adequate job with deep-dive analysis into the individual technology silos, there has remained a gap in the overall approach to providing an integrated and holistic view of IT operations within the mainframe world.

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. Tera-bytes 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. Every transaction across CICS, Db2, and WebSphere MQ results in an SMF log record being created. And it doesn't end there: anything that occurs on z/OS -- network activity, file transfer operations, and more -- has some type of related log information that can be used to gain operational intelligence.

The challenge has been — how to easily extract and analyze this data to answer the questions that need to be answered. Today most organizations must rely on a variety of tools and processes to answer some of the critical questions related to the health and security of their mainframe infrastructures:

- **What is the health** of my IT infrastructure?
- **How well are my** applications performing?
- **What problems** are impacting availability?
- **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?

In this eBook we will take a look at some of the types of things that can be monitored along with sample dashboards that demonstrate these capabilities. We'll call this our IT Operations Checklist for z/OS mainframes, and although it is not the entire list, it is a comprehensive start to ensuring the health, availability, and security of z/OS mainframe systems.





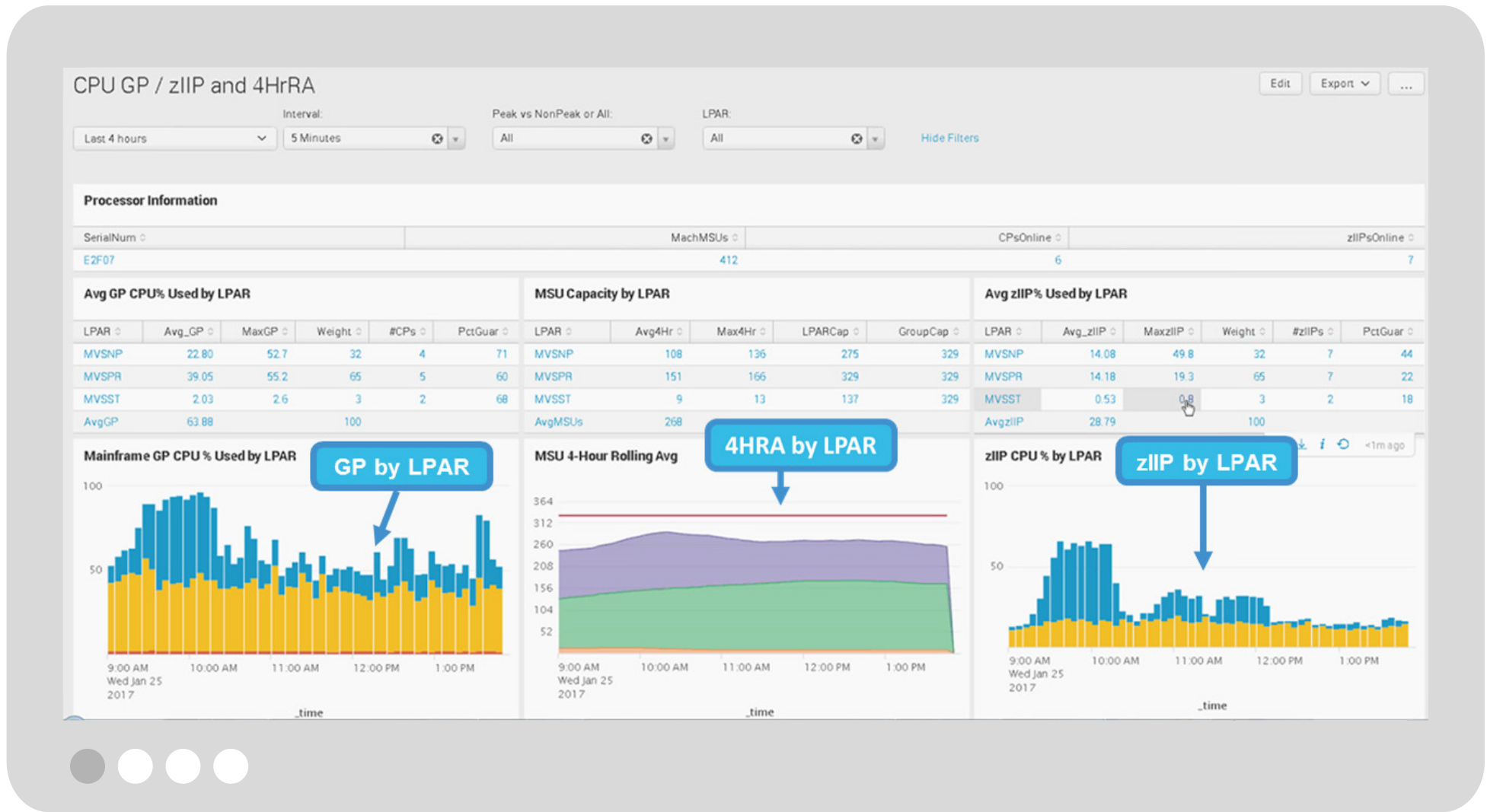
# IT Operations Checklist for z/OS Mainframes

## 1. Monitor System Performance

Monitor all critical resources for a z/OS LPAR including CPU utilization, memory, common storage utilization, and paging rates to ensure business services are not impacted.

Determine if specialty processors (zIIPs) are being used to reduce general processor utilization by monitoring the CEC MSU capacity alongside the 4-hour rolling average (4HRA) utilization for each LPAR.

Get visibility into z/OS RMF III Monitor data to assist with business decisions related to hardware resource consumption and utilization.





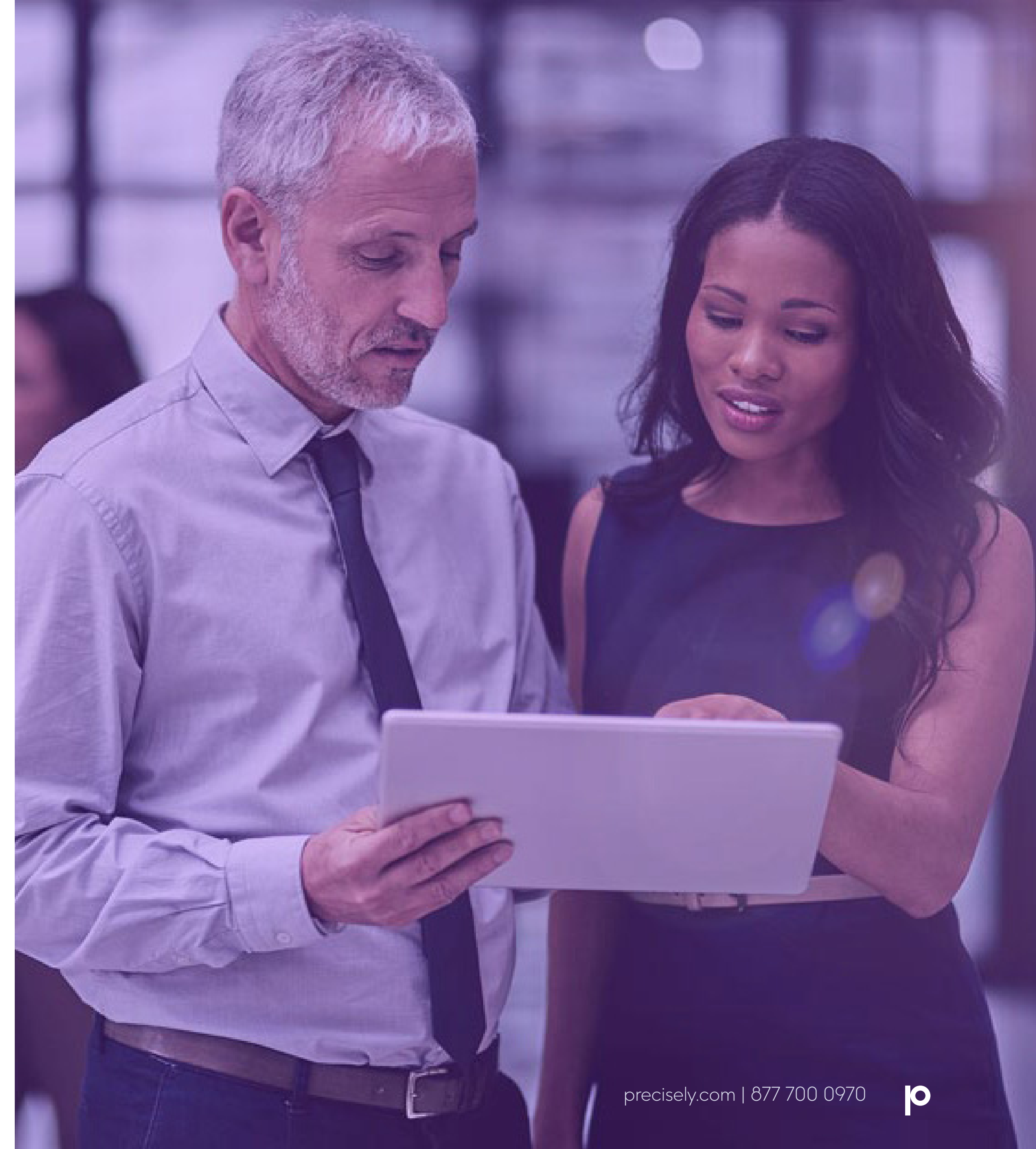
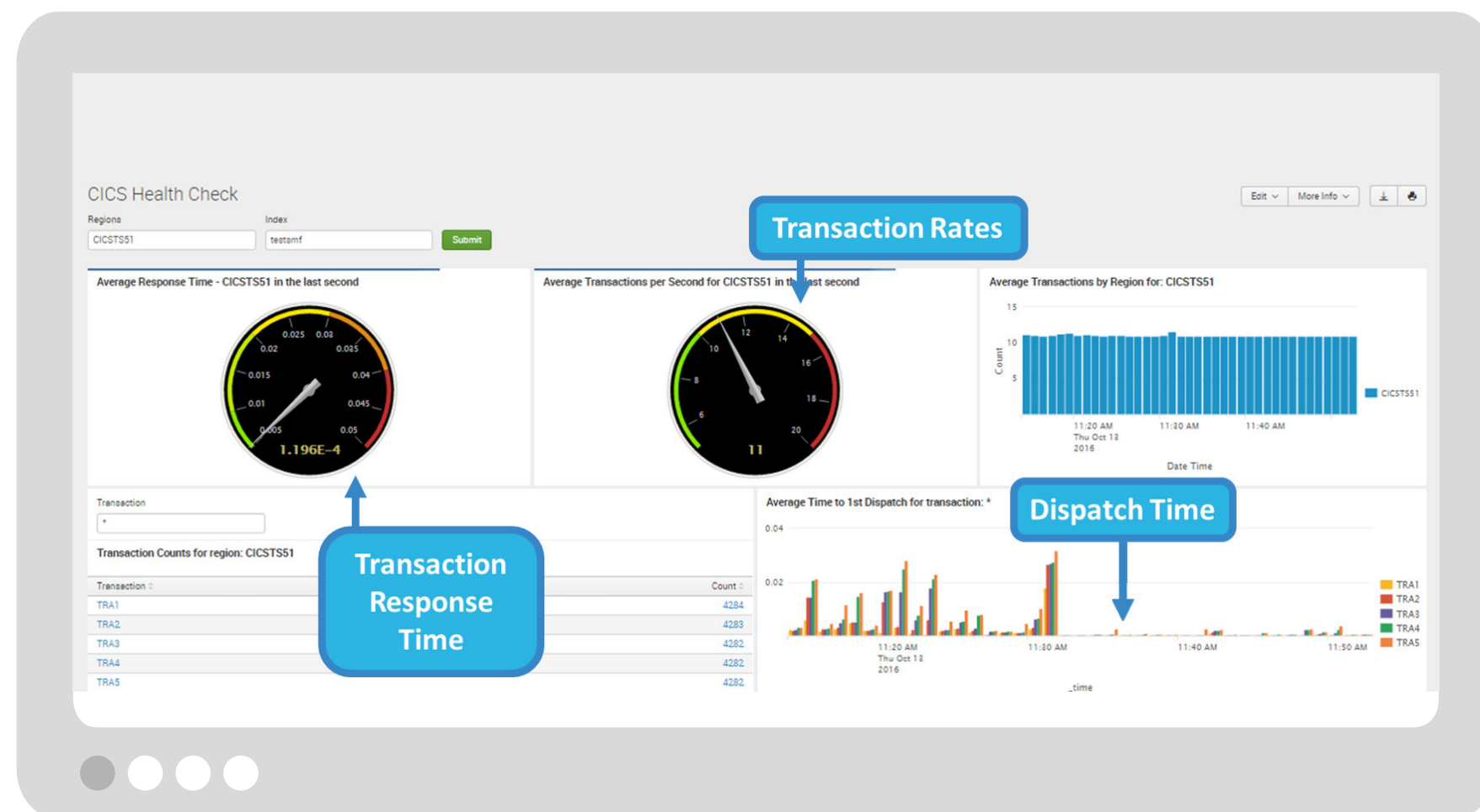
# IT Operations Checklist for z/OS Mainframes

## 2. Monitor Critical Sub-systems

### A. CICS Health Check

Monitor CICS regions and transactions supporting critical business services including identifying transaction failures that are impacting business services.

Get visibility into CICS key performance indicators including transaction rates, dispatch times, abends, CPU utilization and response time to determine if business services are being met or impacted.



# IT Operations Checklist for z/OS Mainframes

## B. Db2 Health Check

Monitor applications that use Db2 on z/OS and identify when Db2 is a contributing factor to the degradation of their performance.

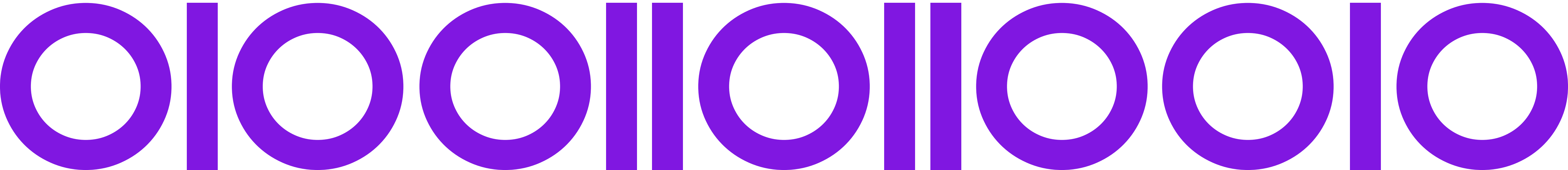
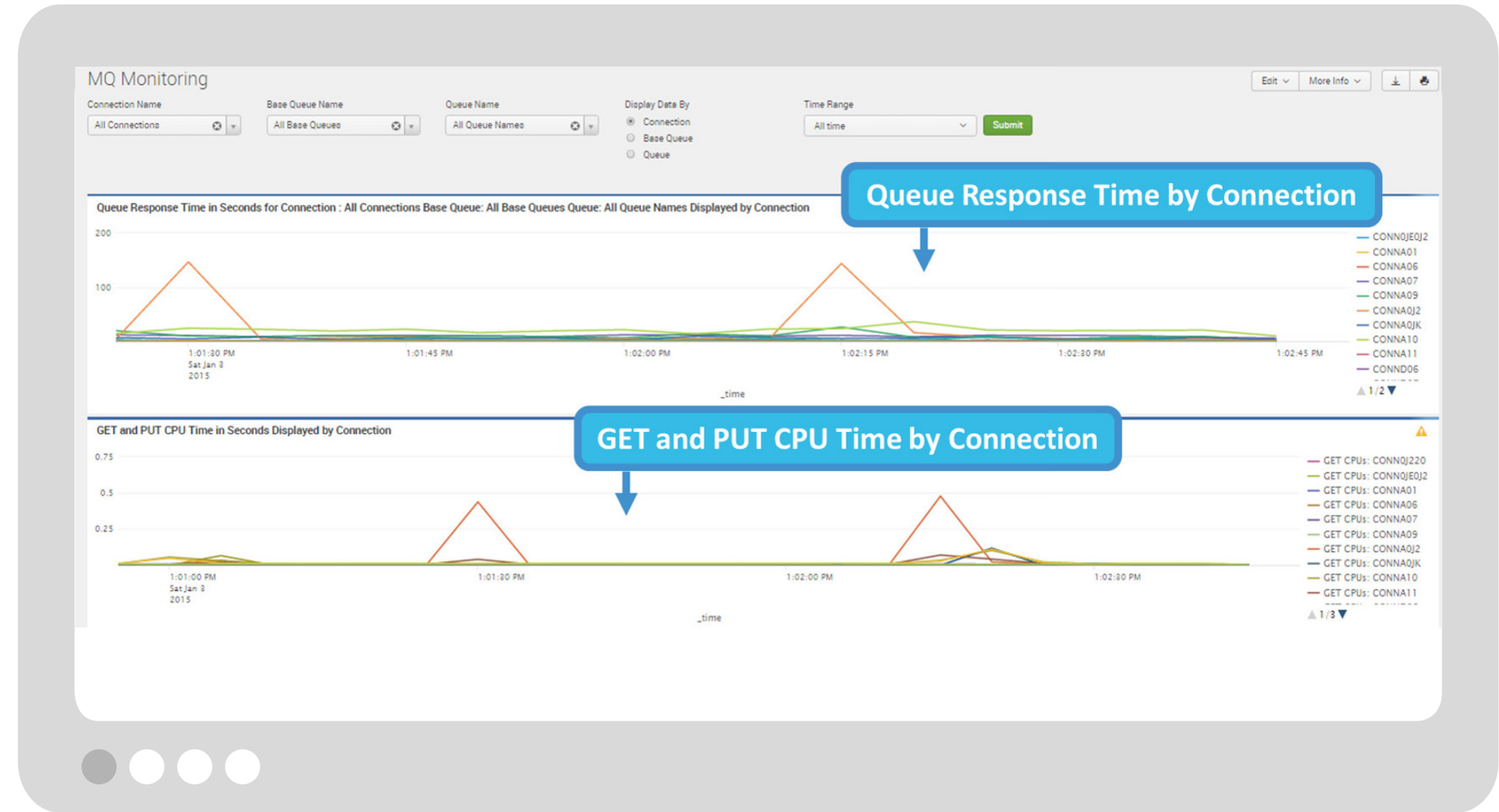
Get visibility into Db2 key performance indicators including lock and resource contention issues.



## C. Websphere MQ Health Check

Monitor WebSphere MQ connections and queues supporting critical business services.

Get visibility into message rates, response times, resource utilization, and queue depths to determine if business services are being met or impacted.





### 3. Monitor Batch Job Execution to Ensure SLAs are Met

Get visibility into batch job performance metrics including runtime, average runtime, start and end times, return codes, and SLA attainment projections.

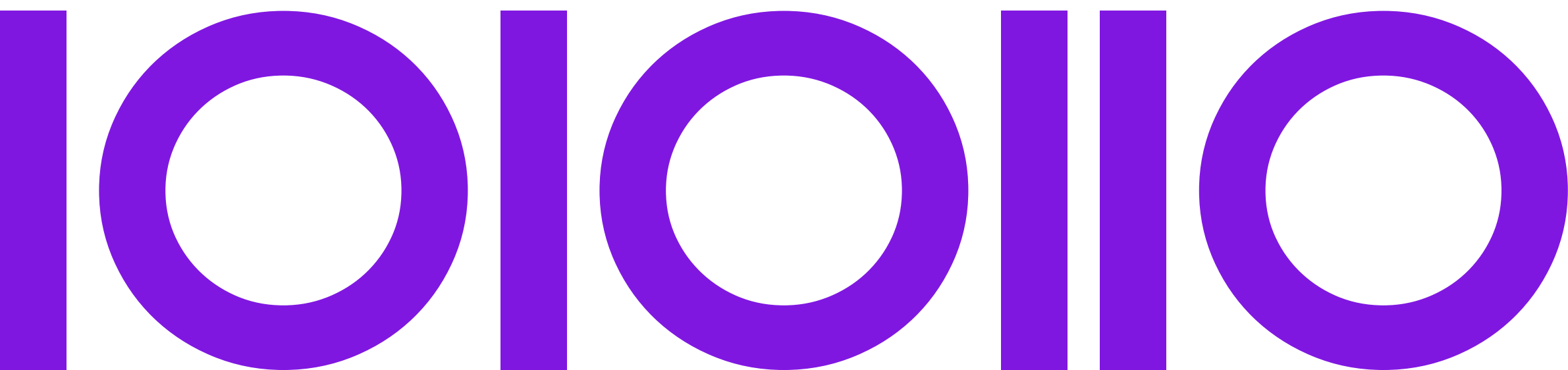
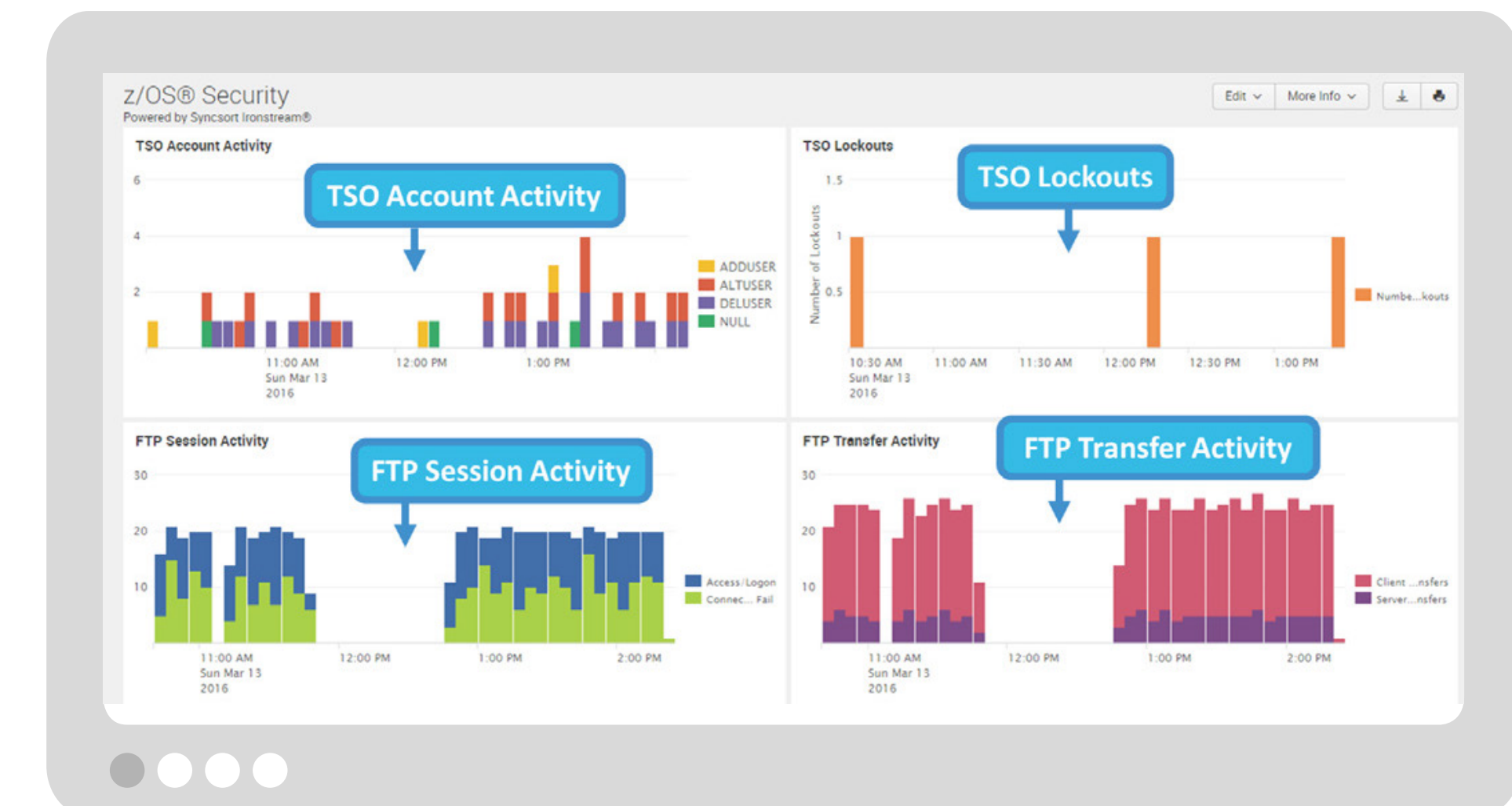
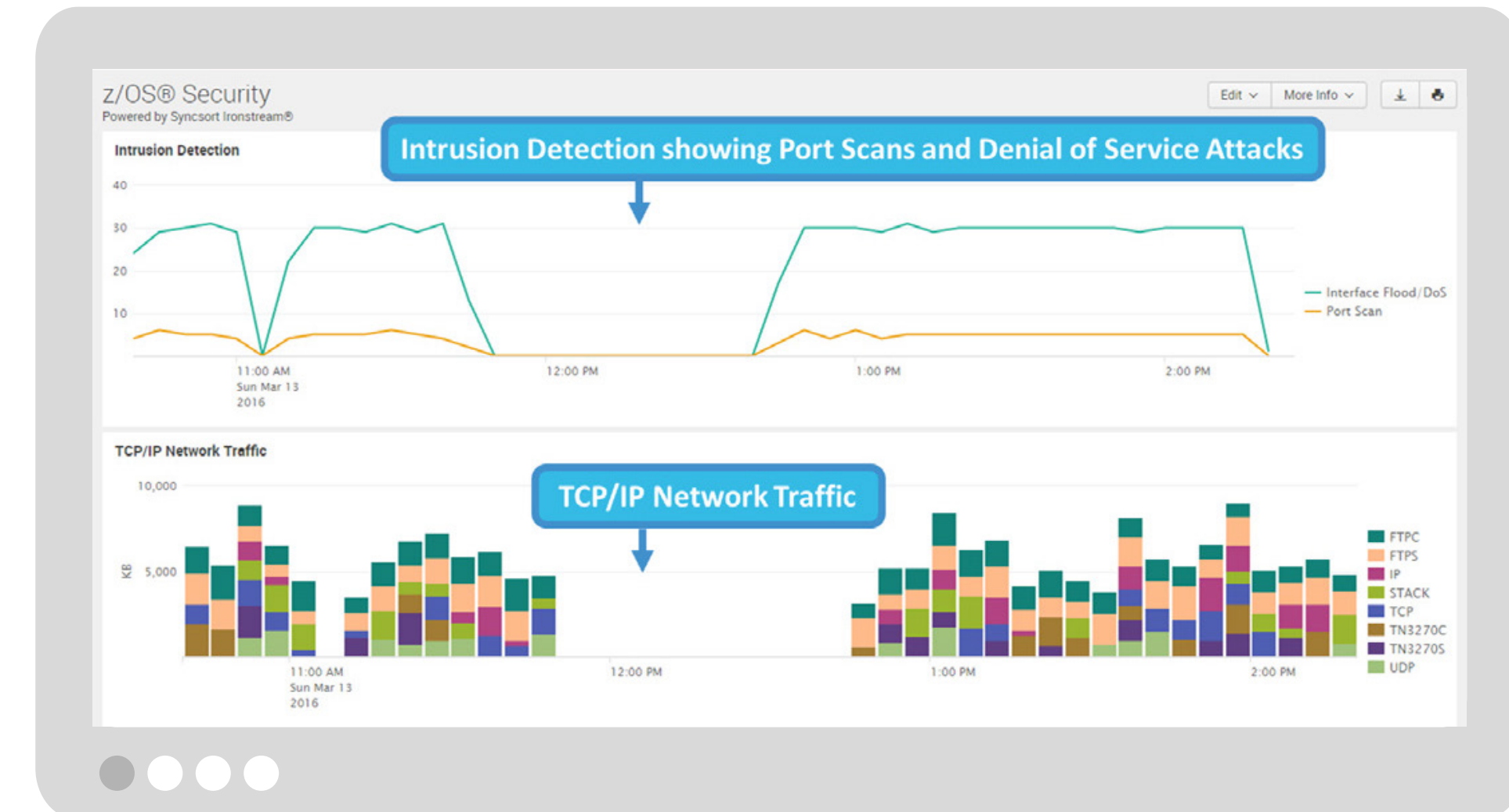
## 6 IT Operations Checklist for z/OS Mainframes

# IT Operations Checklist for z/OS Mainframes

## 4. Monitor Security Information and Events

Monitor key security information and events within z/OS to determine potential threats and security breaches including:

- **Monitor data movement** based upon inbound and outbound FTP operations.
- **Monitor dataset access operations** to determine potential security threats based on unauthorized access attempts, as well as to ensure that only authorized users are accessing secured information.
- **Monitor privileged and non-privileged user activity** to detect unusual behavior patterns such as off hour connections or a high number of invalid logon attempts and other authentication anomalies.
- **Analyze network traffic** for unexpected high data volumes from a device/server, port scans, floods, and potential intrusions.





# Conclusion

New technologies and products have emerged that enable organizations to capture mainframe information and quickly move it to an open-system based analytics platform where it can be integrated, correlated, and analyzed to detect for anomalies and issues, and visualized in a format that is familiar and comfortable for today's IT workforce. Analytics solutions can be used to address gathering all the data sources required to satisfy an IT Operations Checklist for z/OS systems. Furthermore, these platforms provide the additional benefit of having a one-stop shop for all the information instead of having to utilize different tools for each technology silo.

Precisely Ironstream is the industry's leading automatic forwarder of z/OS mainframe operational data to analytics platforms. Ironstream gathers all the required data sources needed by z/OS customers to analyze and visualize information to support a comprehensive IT Operations Checklist.



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

- Get better visibility into the health and availability of their IT infrastructure.
- Achieve higher operational efficiency.
- Perform better problem-resolution management.
- Ensure healthier IT operations.
- Map critical services to 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.





## 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](https://www.precisely.com).

[www.precisely.com](https://www.precisely.com)

Copyright ©2020 Precisely. All rights reserved worldwide. All other company and product names used herein may be the trademarks of their respective companies.