
# Mainframe Event Acquisition System™ (MEAS™)

**Does your SIEM strategy encompass your company's mainframe? Or, is it limited to Windows, Linux and UNIX platforms? No existing SIEM platform on the market today was designed specifically for the z/OS operating system -- this represents a conspicuous 'gap' in your compliance strategy. And this gap, if not quickly remedied, could put your company at considerable risk. However, by handling your mainframe data in a proactive, secure manner, you can maximize your security and compliance strategy.**

**Introducing the Mainframe Event Acquisition System™ (MEAS™).** MEAS™ was designed from the ground up to enable mainframe users ***to collect, store, report and analyze data real time***, through seamless integration with commercial Event Management (EM) and Security Information and Event Management (SIEM) technologies like McAfee ePolicy Orchestrator (ePO), McAfee Nitro, HP ArcSight, IBM Q1 Labs and others.

The z/OS platform is not going away like many predicted. Seventy percent (70%) of all business data is still processed by a mainframe. Increasingly, mainframes are subject to compliance requirements and increased scrutiny requiring the collection of events and logs real time from the mainframe. The SIEM technologies were not designed to collect mainframe data real time at the level of detail needed to meet regulatory compliance requirements.

MEAS™ is designed to monitor your events on your z/OS platform real time in the same way you are monitoring your distributed environment. MEAS™ will detect 'suspicious' activities before they take you 'out of compliance' and subject your company to fines and penalties. The product can be configured to generate a full complement of packaged reports for the CCO/CSO/CRO/or the CISO. No other product on the market focuses exclusively on mainframe exposure and risk. Once installed, MEAS™ customers can rest assured that their mainframe systems are just as secure and compliant as their Windows, UNIX, and Linux counterparts.

## What is the cost of a security breach to your organization?

- Seventy percent (70%) of all business data is still processed on a mainframe every day
- Average cost per identity: $117(1)
- Average record stolen per breach: 99,000(2)
- Average cost per company: $11,572,532

(1)Allied World Data Loss Calculator
(2) Ponemon Institute

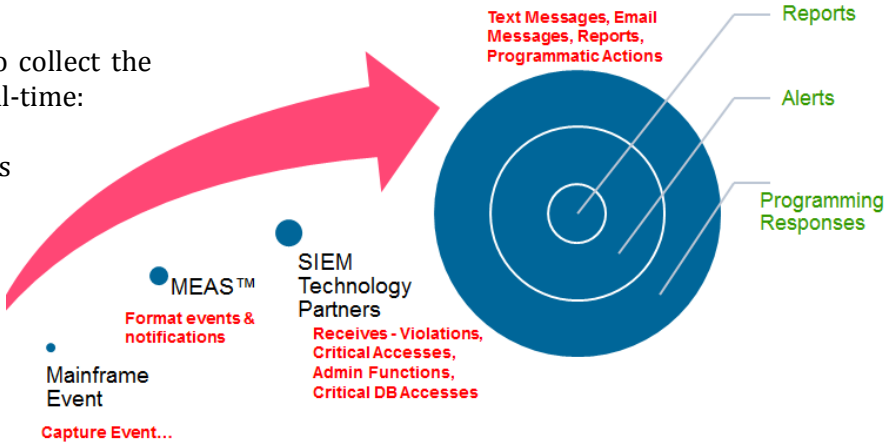
## Maximize your security and compliance with MEAS™

- Real-time mainframe event management
- Integrated with all leading SIEM vendors
- Know about it WHEN it happens
- Find that 'needle in the haystack'

MEAS™


MEAS™ was designed to allow users to collect the following types of mainframe events real-time:

- RACF, TSS, ACF-2 Security events
- Dataset activity
- Database events
- Transaction processing events
- FTP activity
- z/OS console messages
- Job abend events
- CA Top Secret audit file activity
- z/OS performance data
- And much more…




## How it Works

MEAS™ listens for events on the mainframe within each LPAR, selecting only those required by the client. When a desired event is detected, MEAS™ will capture the event details; convert the data to expose the event to the EM and SIEM technology already installed by the customer. Additionally, MEAS™ can write and keep a history of events in an SQL database that can be used to execute queries against the data, perform event correlation and send additional events to the EM and SIEM software for remediation.

By leveraging your existing SIEM platform to manage your mainframe events along with the rest of your IT infrastructure, you can save money on hardware, software and save time. By having real-time access to your mainframe events, you can better react to situations that require your attention. No more running batch jobs to search through SMF data and having to wait 24 hours to discover a potential breach or out-of-compliance condition. With MEAS™, you will know about and be able to quickly respond to events that could have a negative impact on your security and compliance policies.

## Features

- Granular event selection criteria
- Multiple event input methods:
  - SMF (Security, Data Sets, Database, CICS, RMF and more)
  - z/OS System Console
  - TSS Audit file
- Retroactive reporting
- Monitor multiple LPARS concurrently
- Optional Microsoft SQL Server standalone database
- Optional McAfee ePO Security Management software

## Specifications

- Supports z/OS Operating Systems
  - z/OS 1.8 and above
- Supports Windows Operating Systems
  - Windows Vista (32 & 64 bit)
  - Windows 7 (32 & 64 bit)
- Supports commercially available Log and SIEM technologies

**Call us for a free 30-day trial!**

**703-825-1202**
**813-258-0488**
**sales@meas-info.com**

MEAS™