

# IronSphere Inspector for Z/OS.

## Automate z/OS STIG Compliance Through Continuous Security Monitoring

When your business needs to meet demanding federal regulations and industry standards, but you rely on manual processing for security scans and auditing, proving compliance can be an ongoing chore of enormous time and effort.

IronSphere is your solution to continuously monitor the mainframe, automate security checks, and initiate reporting – and then help simplify auditing to prove compliance. What could take months to examine manually, IronSphere can automate in a few minutes, with low overhead and real-time results.

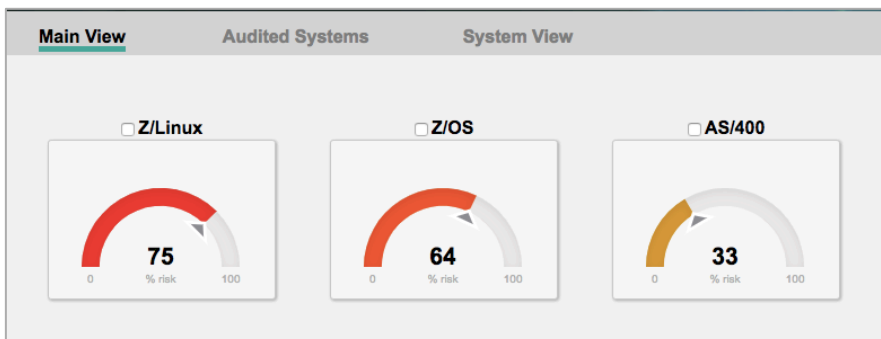
Security scans are based on DISA STIGs (Security Technical Information Guides from the Defense Information Systems Agency), which contain optimized policy and configuration information for system applications.

IronSphere automatically compares each application to its STIG to find system vulnerabilities, altered system settings, modified operands, and other discrepancies. If an issue is detected, IronSphere launches automatic diagnostic routines to determine:

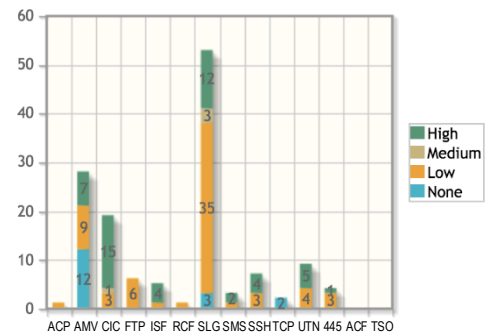
- Security problems and errors
- Which components are affected
- Root cause of any problem
- Which issues are the highest risk

The resulting real-time report identifies errors, assigns risk levels, and charts the findings. It even describes how to resolve the problem.

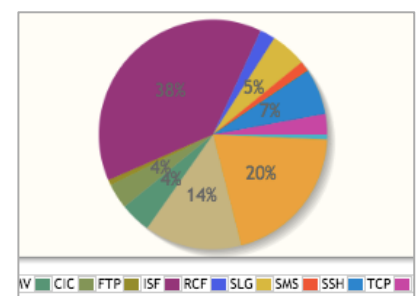
*A dashboard reports the health of each system with intuitive, color-coded graphs.*



- Real-time vulnerability reporting.
- Mainframe DISA STIG monitoring.
- Risk resolution sent to your inbox.
- Simplifies complicated mandates.
- Easy z/OS security audits.



*Risk levels within each group.*



*Distribution of a risk level across groups.*

Data is displayed graphically in easy-to-understand charts and tables. Results can be sorted and filtered per system, LPAR, group, severity level, or other criteria.

# Simplify mainframe security! Intuitive IronSphere GUI gives you the problem resolution.

Name	Severity	Details
MVS-AMV-040-00	Low	Inaccessible AFP libraries defined.
MVS-AMV-160-00	Medium	Inapplicable PPT entries have not been
MVS-AMV-325-00	None	Non-existent or inaccessible Link Pa
MVS-AMV-350-00	None	Non-existent or inaccessible LINKS
MVS-AMV-410-00	None	Database is not on separate pr
MVS-AMV-440-00	None	SSWORD data set and OSpassword
MVS-ACP-010-00	Medium	SYS1 PARMLIB is not limited to only
MVS-ACP-020-00	None	Access to SYS1 JARCS is not prop
MVS-ACP-030-00	None	Write or greater access to SYS1 SVC
MVS-ACP-040-00	High	Write or greater access to SYS1 IMA

Security and GRC teams are z/OS risk-aware :

Automatic assessments detect changes in the status of system components, identify risk levels, and report all results from a single graphical interface.

IronSphere can conclusively prove an application is error-free and in compliance with security standards.

IronSphere can validate that an application or group meets security standards and a log history can conclusively prove system integrity and continuous monitoring.

Results are retained within the IronSphere server, allowing auditors easy access for compliance verification.

IronSphere is an open architecture product that allows client development of checks, triggers and parmlib directives, supporting all three ESMS: RACF, Top secret and ACF2.

A dashboard reports the health of each system with graphs for any level of user, regardless of mainframe expertise. Results can be shown in a variety of comparison and history charts to suit the needs of any management or security team.

Each IronSphere agent reports diagnostic results to the secure server over HTTPS. Messages and trace data are not stored on the mainframe.

Name	Severity	Details
MVR-RCF-480-00	High	The PROTECTALL SETROPTS value specified is improperly set.

**Information**

Name	MVSA
Type	z/OS 02.02.00 HBB77A0
Class	Data Integrity
Description	When PROTECTALL processing is active and set to FAIL, the system automatically rejects any request to create or access a data set that is not RACF protected. Temporary data sets that comply with standard MVS temporary data set naming conventions are excluded from PROTECTALL processing. PROTECTALL requires that data sets be RACF protected. In order for PROTECTALL to work effectively, you must specify GENERIC to activate generic profile checking. Otherwise, RACF would allow users to create or access only data sets protected by discrete profiles. The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP provides the ability to set a number of these fields at the subsystem level. If no setting is found, the system-wide defaults will be used. The improper setting of any of these fields, individually or in combination with another, can compromise the security of the processing environment. In

**Fix**

Evaluate the impact associated with implementation of the control option. Develop a plan of action to implement the example below: The RACF Command SETR LIST will show the status of RACF Controls including the value for the PROTECTALL is ACTIVATED and set to FAIL by issuing the command SETR PROTECTALL(FAIL).

Detailed STIG information is displayed in one location, including the fix.