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.

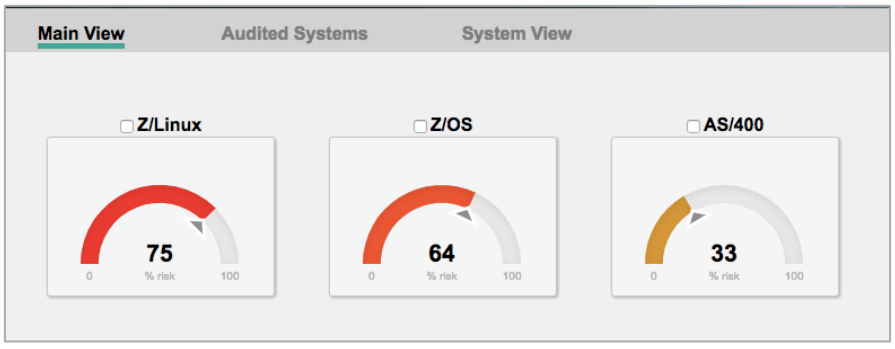
Security scans are based on DISA STIGs (Security Technical Information Guides from the Defense Information Systems Agency), which contain optimized policy and configuration information for system applications.

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.



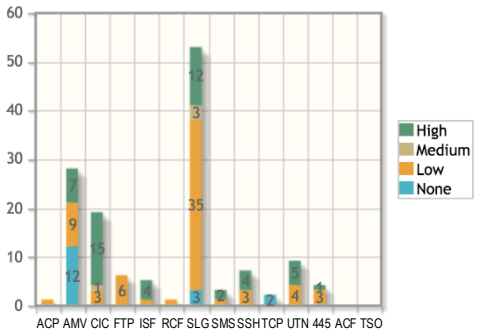
Real-time vulnerability reporting.

Mainframe DISA STIG monitoring.

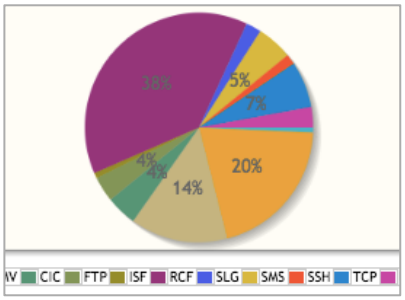
Risk resolution sent to your inbox.

Simplifies complicated mandates.

Easy z/OS security audits.



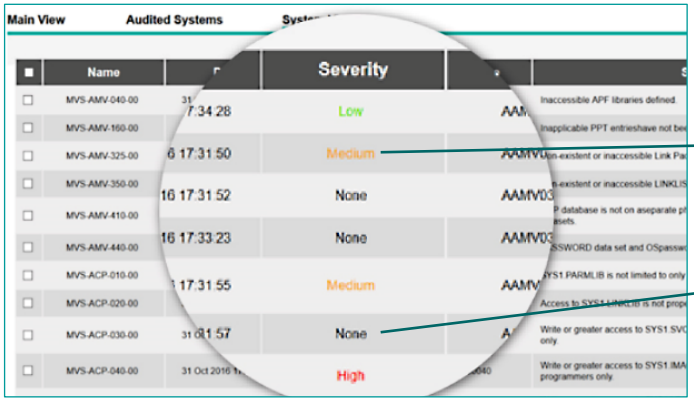
Risk levels within each group.



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.



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.

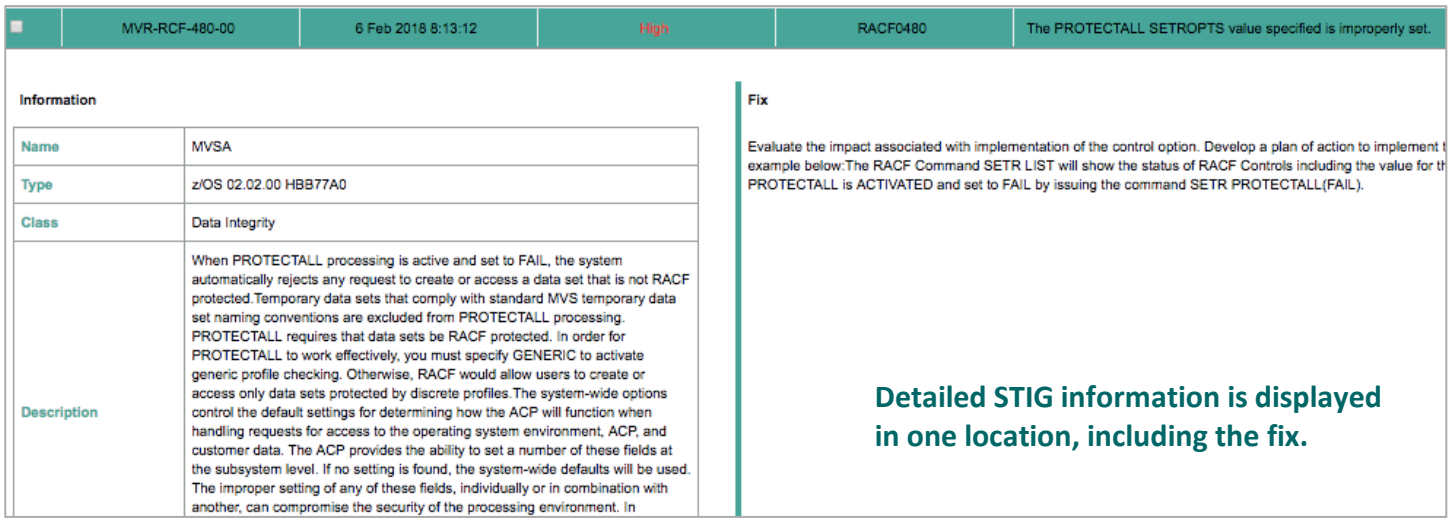
IronSphere can validate that an application or group meets security standards and a log history can conclusively prove system integrity and continuous monitoring.

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.



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