SDS IronSphere for z/OS

Automate z/OS STIG Compliance through Continuous Security Monitoring

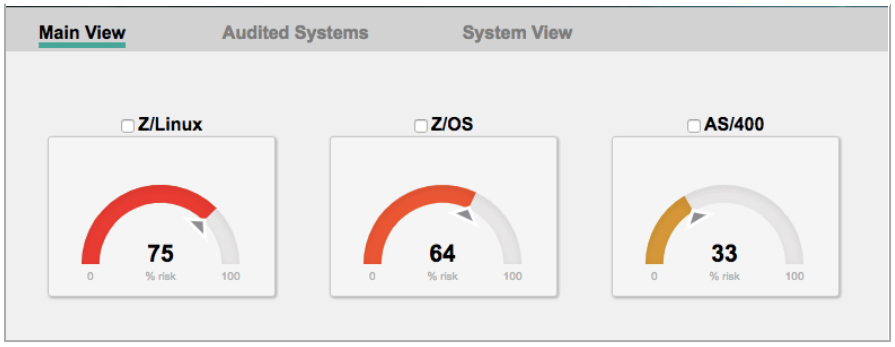
Mainframes are heavily used by high-volume businesses required to comply with stringent federal regulations and rigorous industry standards. They are also often run by outdated enterprise clients that rely on costly manual processing. For a system with numerous servers or LPARs, security scans can be an ongoing chore of enormous time and effort.

IronSphere conquers the task. It continuously monitors the mainframe, automatically performing security checks and looking for system vulnerabilities, altered system settings, and modified operands. What could take months to examine manually, IronSphere can automate in a few minutes, with low overhead and real-time results. If a change is detected, IronSphere launches automatic diagnostic routines to determine:

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

Security scans are based on IBM z/OS RACF® or CA Top Secret® STIGs (Security Technical Information Guides) which contain optimized policy and configuration information. IronSphere automatically compares each application to its STIG to detect discrepancies. 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.



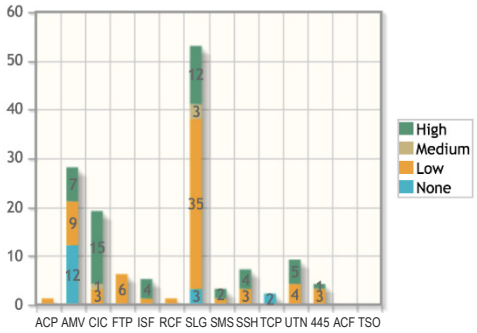
Real-time vulnerability reporting.

Mainframe STIG monitoring.

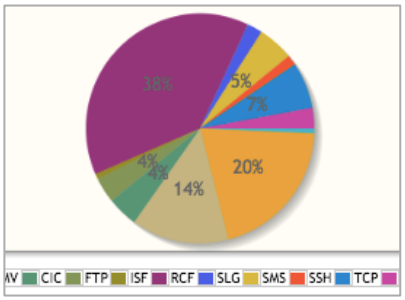
Risk resolution sent to your inbox.

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.

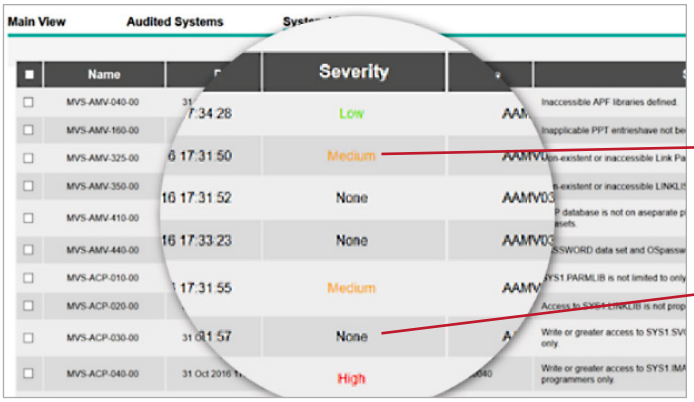
Compliance, Continuous Monitoring, and Data Protection

IronSphere helps comply with GDPR, NIST ISCM, and DoD requirements.

DATASHEET

SDS
DO MORE WITH LESS

Simplify mainframe security! Intuitive 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.

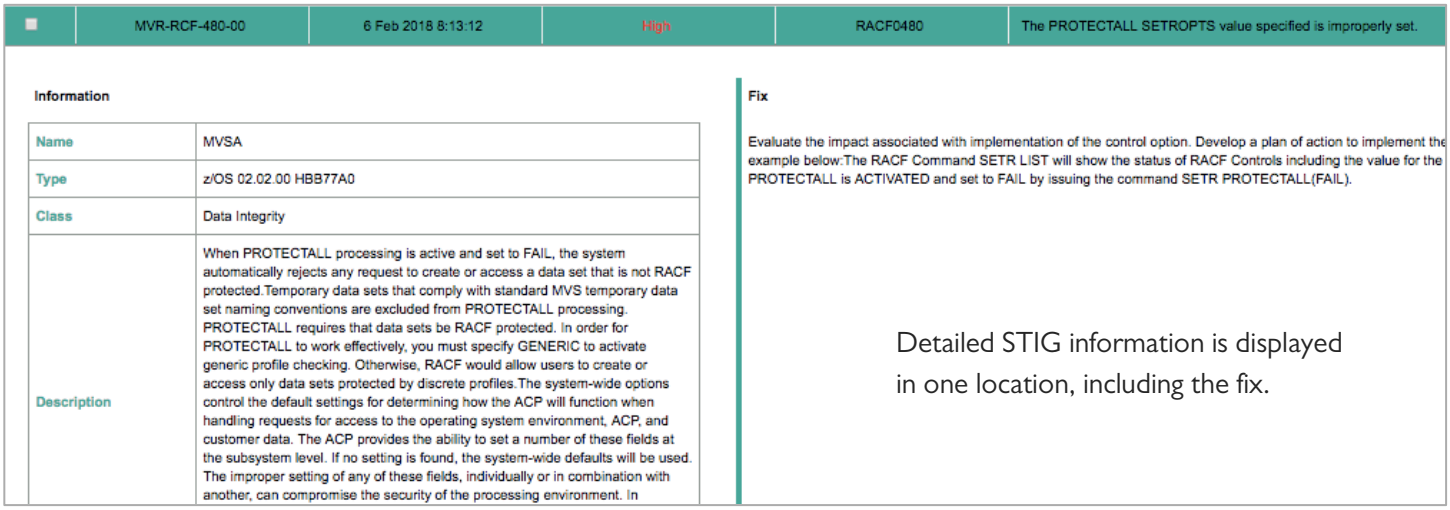
IronSphere can conclusively prove an application is error-free and in compliance with security standards.

IronSphere can validate that an application or group meets security standards.

When run regularly over time, a history is created that can confirm system integrity for compliance reporting.

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 results to the server over HTTPS. Messages and trace data are not stored on the mainframe.



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

About SDS

Founded in 1982, SDS supports over 25 products for z/OS, MVS, VSE, VM, AIX, Linux, and Windows. SDS has licensed more than 1,000 enterprise clients worldwide with quality mainframe software and offers award-winning technical support. Comprehensive solutions focus on security, encryption, data compression, and network monitoring. To learn more, please visit our web site.