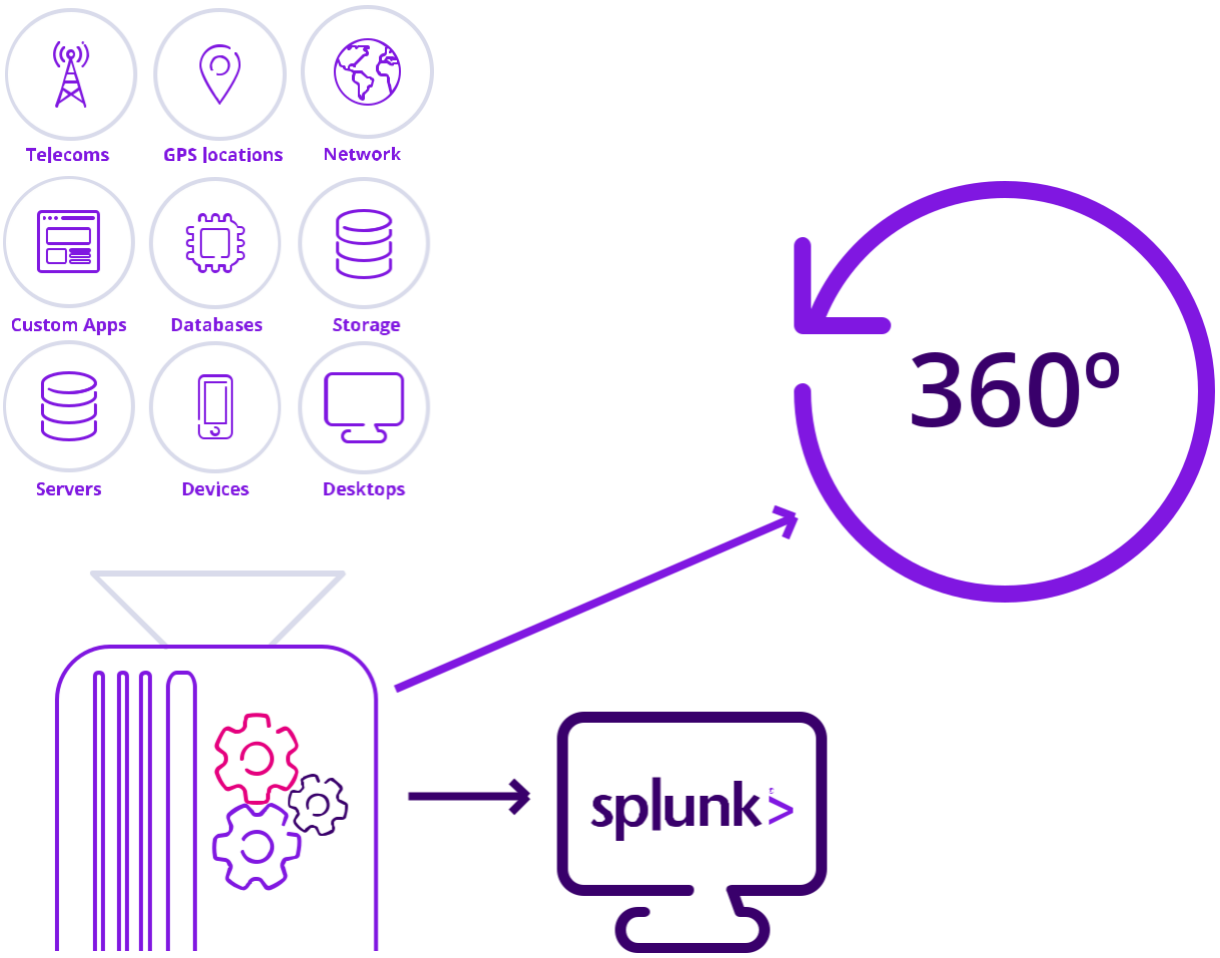
Ironstream for Splunk®

Integrating your critical security and operational machine data from IBM mainframe and IBM i systems into Splunk for a complete picture of your IT environment

Ironstream was developed with Splunk to solve the challenge of making complex mainframe and IBM i data available for true enterprise-wide analytics. Splunk is the IT platform for monitoring, integrating, analyzing, and visualizing security data from across the enterprise. Ironstream for Splunk integrates critical security and operational machine data from IBM mainframe and IBM i systems into Splunk for a complete picture of the IT environment. It delivers real-time, total visibility to machine data without the need for redundant or specialized IBM mainframe or IBM i expertise.

Ironstream makes it simple to securely collect, transform and forward log data from traditional IBM systems to Splunk where its merged with machine data from across the IT infrastructure. It is the industry's leading automatic forwarder of z/OS mainframe log data and IBM i machine data to Splunk Enterprise. It seamlessly integrates all critical IBM mainframe and IBM i data sources into Splunk to support strategic enterprise-wide initiatives such as Security Information and Event Management (SIEM), IT Operations Analytics (ITOA), and IT Service Intelligence (ITSI).



Key Features

Support data model for mainframes

- Splunk Macros help locate data
- Splunk Event Types can categorize data
- Security information from ACF2, RACF, and Top Secret
- 'Bakes-in' SME knowledge

Maintain valuable data with Splunk applications

- Splunk Cloud and Splunk Enterprise help collect envision as well as reports of log data
- z/OS log files such as WebSphere, Log4j, Syslog

Support enterprise security for organizations

- Protect data against security breach
- Allow users' complete access to security alerts and risks on systems
- Splunk Enterprise Security application gives total visibility to threat indicators such as unusual movement of data
- Organizations can see, analyze, and correlate all relevant data including SMF records from RACF

Support for all critical IBM mainframe z/OS data sources

- IMS log data
- SMF and Syslog records
- Security information from RACF, ACF2, and Top Secret

Support for all critical IBM i data sources

- Operating System
- Message Queue Data
- History Log
- System Performance
- Custom Data

Promote easy integration of data with Splunk applications

- Secure integration of data into many customizable dashboards
- Detailed visualization of potential threats and anomalies across entire IT infrastructure
- Total visibility ensures effective deliver of IT services by businesses

* IBM mainframe only

Support simple real-time, 360-degree intelligence

- Collect log data from traditional IBM systems and forward the data in real-time to Splunk
- Users can search, analyze, and visualize the mainframe and IBM i data

Support for operational insights and efficiency

- ITOA helps correlate events across every system in the enterprise increasing efficiency and cost-saving
- Ensures critical processing resources are utilized to their maximum potential

Benefits

- IBM mainframe and IBM data are integrated into Splunk to remove blind spots in IT analytics
- Enables 360-degree view of IT environment for operational analytics
- Accelerate problem resolution with total visibility access to traditional IBM systems
- Deliver security information for visibility into enterprise-wide security threats and incidents
- Improved operations help spot problems before they start, resolve outages quickly, and optimize infrastructure spend
- Provide faster insights by sharing critical, real-time insights across the enterprise

Ironstream for Splunk enables organizations to integrate critical security and operational machine data from mainframe and IBM i systems into Splunk for a complete view of the IT environment.