syncsort

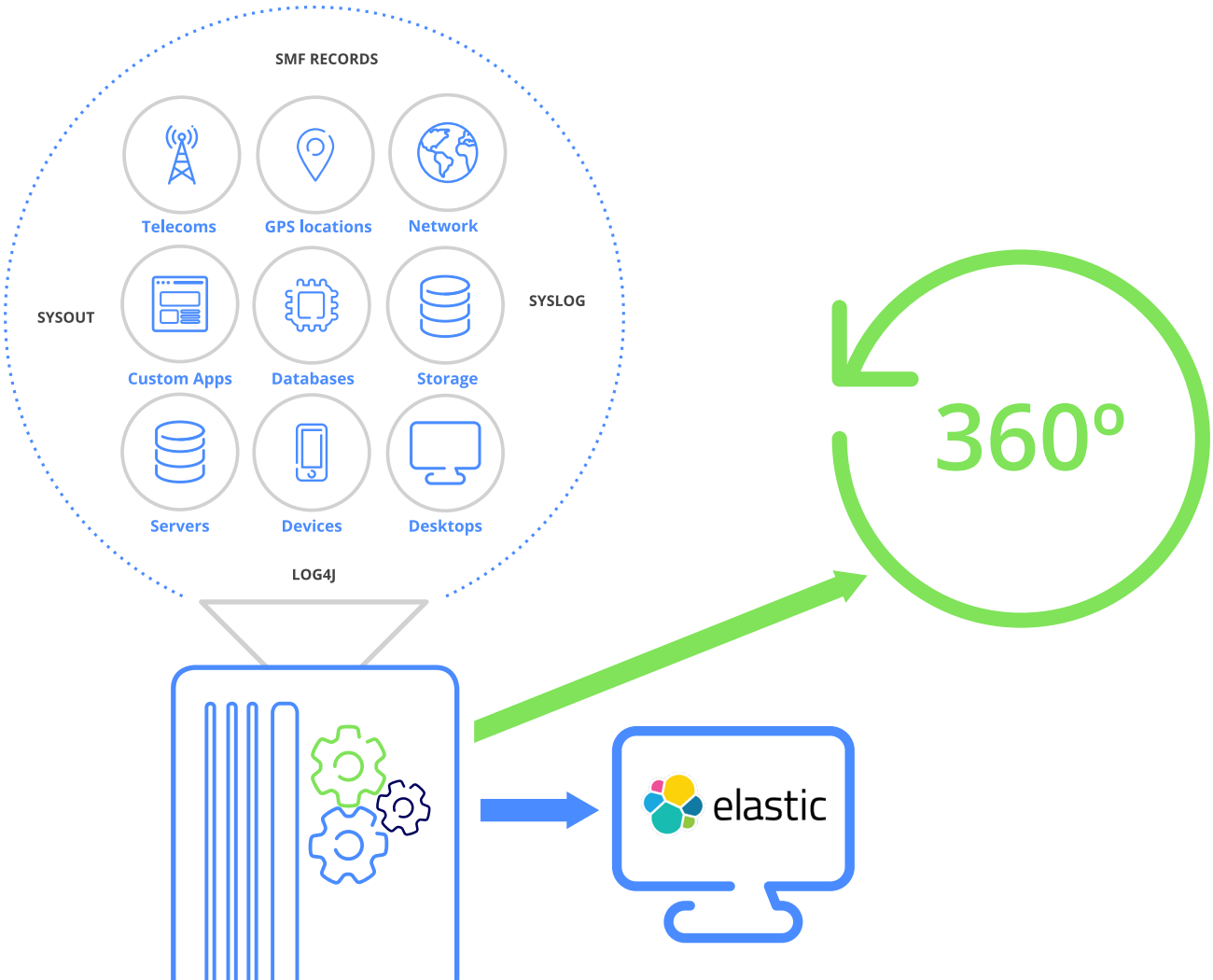
SOLUTION SHEET

Ironstream for Elastic®

Integrating your critical security and operational machine data from your mainframe into Elastic for a complete picture of your IT environment

To manage today's IT infrastructure, you need to have a single, comprehensive view of all the systems in your environment. Elastic has become a popular open-source option as the IT analytics for many companies but it does not support collection of machine data from traditional IBM mainframe. Ironstream for Elastic makes it simple to collect, transform and securely stream data from these traditional IBM platforms into Elastic with no need for mainframe expertise.

Ironstream is the industry's leading automatic forwarder of z/OS mainframe log data (i.e., SMF records, SYSLOG, RMF data, IMS data, log4j records, USS files, SYSOUT, and more) to platforms like Elastic. Mainframe data forwarded by Ironstream can be merged with other machine data from across an organization's IT infrastructure to support enterprise-wide IT Operations Analytics (ITOA), and Security Information and Event Management (SIEM).



Best-in-Class Solution Provides Real-time Mainframe Insights

Ironstream makes it easy and cost-effective for organizations to get a real-time, 360-degree view of their IT infrastructure.

- **Less complexity** breaks down silos and seamlessly integrates with Elastic for a single view of all your systems, with no mainframe expertise required.
- **Clearer, more precise security information** with complete visibility into enterprise wide security alerts and risks for all systems, including mainframes.
- **Healthier IT operations** because anomalies in the mainframe environment are accessible for analytics and diagnosis along with the information coming from other platforms.
- **Better problem-resolution management** with real-time access to mainframe data sources so you can act fast.
- **Higher operational efficiency** enabled by advanced filtering of SMF records, utilization of zIIP processors, and data loss protection.
- **Visibility into cross-platform transactions** to monitor and improve IT service delivery and application performance.

With extensive support for critical mainframe data sources including Syslog and SMF records, Ironstream enables organizations to keep their IT infrastructure secure and performing at its best.

Key Features

Support for all critical IBM mainframe z/OS data sources including:

- **IMS log data** containing critical information for security and regulatory compliance as well as monitoring performance, capacity utilization, throughput, and resource utilization.
- **SMF and Syslog records** needed for IT operations analytics, Security Information & Event Management, and IT Service Intelligence. Also supports SMF records generated by major software vendors including BMC, CA, and Compuware.
- **Security information from RACF, ACF2, and Top Secret** to monitor intrusion detection, TSO logon activity, TSO account activity, FTP authentication sessions, FTP change analyses, and other critical security information.
- **Resource Measurement Facility III data** captured in real time providing information on potential bottlenecks and performance delays.
- **UNIX Systems Services (USS) and Log4J files** which can contain critical web-application log information coming from IBM WebSphere, as well as other web-based applications.
- **Network-performance data** providing insight into all IP network activity including alerts for network availability, performance, capacity, and messaging.

- **Advanced Filtering of captured SMF data** uses low overhead exits with no log stream dependencies. Filtering reduces data volume and network traffic ensuring that only critical records and fields required for desired analytics and visualization are forwarded.
- **Ironstream API** enables COBOL, REXX, and Assembler applications to directly forward application data to an analytics platform for enhanced visualization of application information.
- **zIIP Processors utilized** to reduce CPU consumption and minimize overhead associated with capturing and forwarding data to analytics platforms.
- **SMF Logstream collection** enables asynchronous collection of SMF data in high transaction rate systems to ensure application performance and low latency.

syncsort