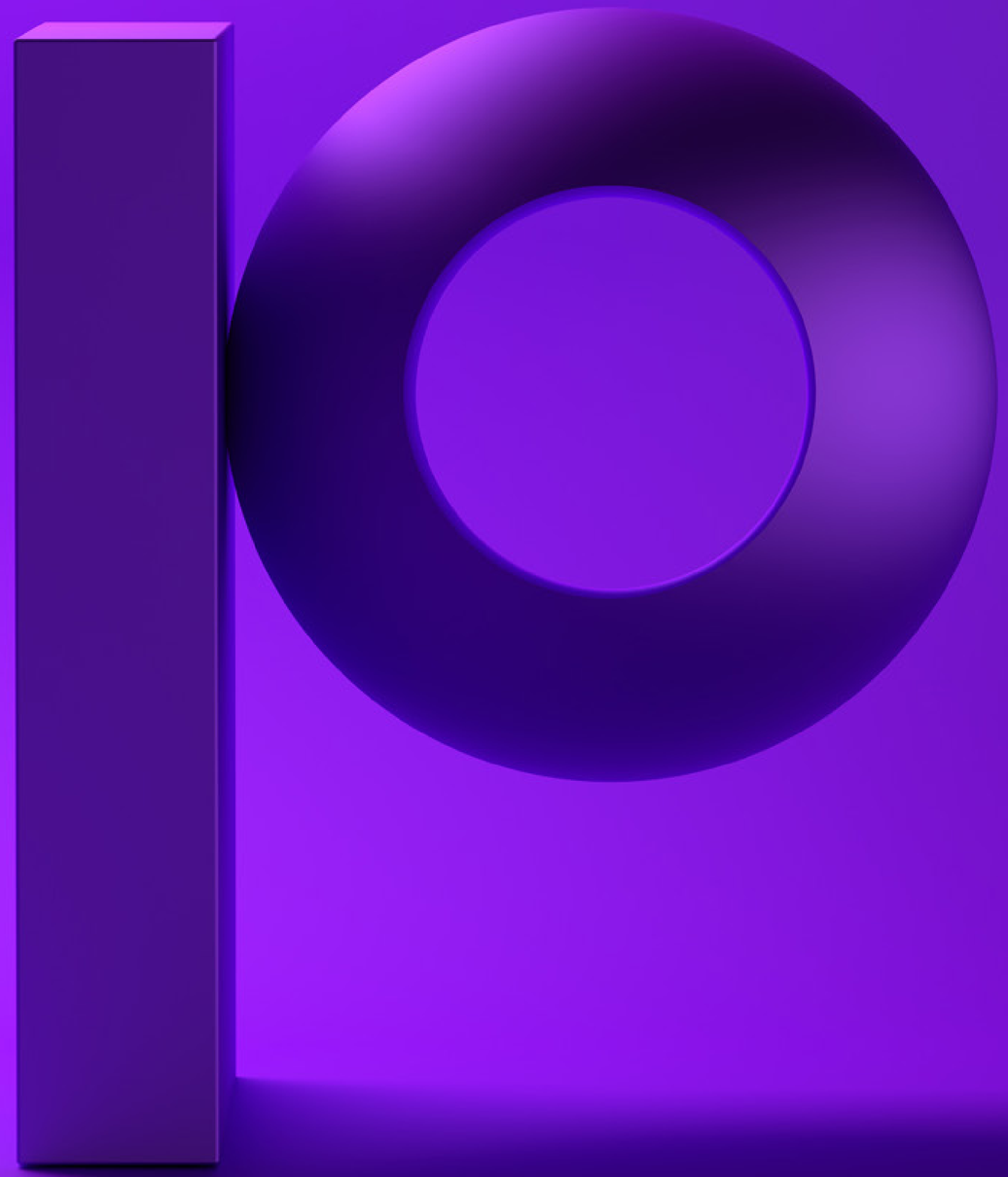
precisely

Top Use Cases for IBM i Data in Splunk: Compliance



Introduction

This is Part 2 in a 3-part series on the use cases for using IBM i Data in Splunk

Data is the most valuable asset that most organizations can have, as it drives strategic business decisions, new product development, customer service and more. However, if not properly managed and secured, data can become a significant liability due to the proliferation of government and industry regulations.

Not only are the number of regulations on the rise, but the rules for complying with each of them is constantly evolving. At the same time, the IT environments in which the data is generated, transmitted, used and stored, is increasing in complexity. This makes it extremely challenging to know what data exists, what type of data it is, where it's located, who is accessing it, and for what purpose it's being used.

Enterprises, and even government agencies themselves, are turning to Security Information and Event Management (SIEM) technology to help face these daunting challenges. SIEM solutions support threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. They also collect, store, analyze, and report on data needed for regulatory compliance to ensure that audit requirements are met as directed.

Because of the complexity surrounding these regulations, regulatory compliance is one of the biggest drivers of SIEM growth. Organizations are investing in SIEMs to help satisfy the requirements created by a long list of regulations and governing bodies, including:

- **PCI-DSS** – data-security standards imposed on the payment card industry
- **GDPR** – regulations to protect the data of European citizens
- **FFIEC** – US Federal standards and mandates imposed on financial services and banking enterprises
- **HIPAA** – regulations imposed by the US Health Insurance Portability and Accountability Act
- **European Banking Authority** – maintains banking regulations addressing AML, payment services and more
- **SOX** – regulations imposed by the Sarbanes-Oxley Act
- **GLBA** – data protection regulations imposed by the Gramm-Leach-Bliley Act
- **FISMA** – data security regulations imposed by the US Federal Information Security Management Act
- **IRS Pub 1075** – one of thousands of IRS regulations, this one mandating how the 50 states must account for unemployment payouts. (See nearby sidebar: "One Compliance Problem Solved"

Implications for IBM i Environments

IBM i systems process massive volumes of critical and sensitive information for enterprises across industries. These organizations are governed by stringent cybersecurity regulations, such as those listed in the preceding section. To stay in compliance and reduce the risk of data breaches and security incidents, all operations on an organization's IBM i system must be continuously monitored.

While IBM i journals and log files are comprehensive, they're also cryptic and voluminous. If information is needed for an audit or analysis, it's nearly impossible to extract it in a timely fashion. Without proper logging and a way to quickly obtain insights or create reports regarding changes to critical databases, enterprises risk failing regulatory audits.

To demonstrate compliance, IT teams need logs and information about a variety of dynamic elements, including:

- Changes to system objects (system values, profiles, creation or deletion of users, authorization lists)
- Sign in and access attempts
- Any action involving sensitive data
- Access to critical databases
- Authentication failures
- Changes to passwords and access rights
- Data transmission and movement

The Role of Splunk

Many organizations are adopting Splunk as their SIEM solution, making it a core component of their security strategy, specifically for integrating, analyzing and visualizing security data from across the enterprise. Not only does Splunk help keep their company secure, but, importantly, it also helps with complex regulatory compliance.

Splunk provides a single platform to operationalize compliance with capabilities to collect, retain, search, alert and report on logs and machine data through an organization's IT infrastructure.

Companies use Splunk to stay ahead of compliance mandates by reducing time, errors and costs with an analytics-driven approach. Splunk offers the benefits of:

- Automated Data Collection: Real-time log and event data ingestion for centralized correlation and analysis
- Continuous Risk Assessment: Granular visibility and real-time insights on information assurance and adherence to controls
- Painless Audit and Reporting: Operators and executives alike can access custom metrics views and ease audit burden via self-reporting

Seamlessly Forward IBM i Logs to Splunk with Precisely Ironstream

Spunk offers a powerful solution for organizations needing to comply with industry and government regulations. However, Splunk does not natively collect essential security and compliance data from the IBM i platform, leaving a significant blind spot and vulnerability. That's where Precisely Ironstream comes in.

Ironstream seamlessly feeds IBM i logs to Splunk, ensuring that critical machine data for the entire IT landscape is available in a single tool. Splunk turns mountains of incomprehensible data into visual insights.

Together, Ironstream and Splunk help organizations achieve satisfactory security and compliance audits, and provide security event tracking, real-time monitoring of security events, automated reporting, and complete visibility into the health and security of all systems in the enterprise.

For more information on getting your critical IBM i data into Splunk, visit www.precisely.com.

precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely's data integration, data quality, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

www.precisely.com