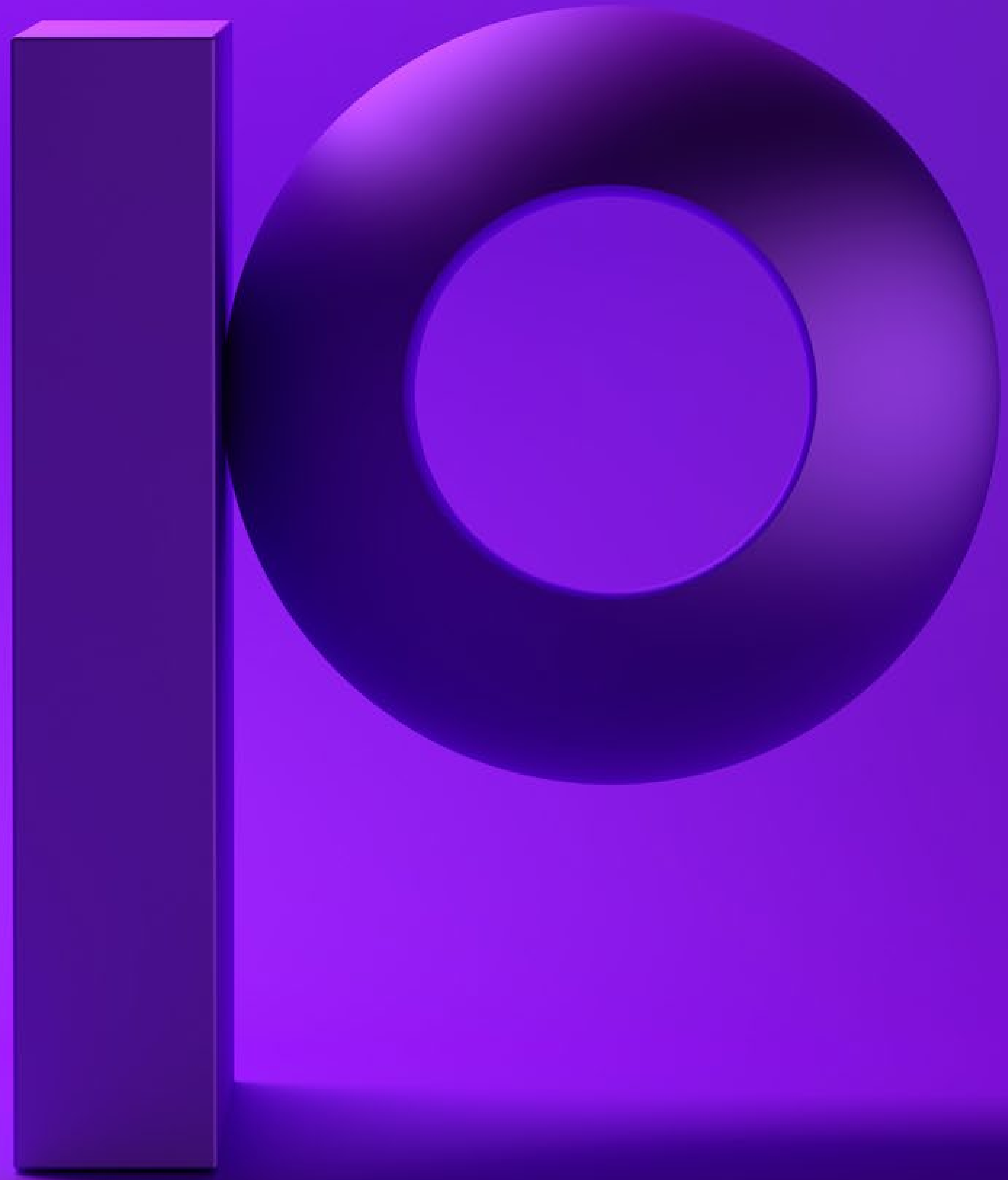
precisely

IBM i Compliance and Security: Identifying the Events That Matter Most with Assure Security and SIEM Integration



Monitoring for Compliance

IBM i systems process massive volumes of critical and sensitive information for enterprises across industries. These organizations are governed by stringent cybersecurity regulations that protect consumers, such as SOX, GDPR, HIPAA, PCI DSS, state privacy regulations, and more. To maintain compliance and reduce the risk of data breaches and security incidents, all operations on an organization's IBM i systems 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
- Powerful user activity, including the commands issued

Monitoring for Security

IBM i systems contain sensitive information that can be extremely valuable and must be protected. Monitoring IBM i system and database changes is critical to preventing, or limiting the damage from, staff seeking to use your data for personal gain and malicious actors from the outside.

The problem is, you won't notice a security incident occurring on your system unless you are reviewing the logs of system and database activity for anomalies, policy violations, and patterns. Without monitoring system activity, you have no way to observe unauthorized activity happening on your IBM i systems, you have no visibility into who's changing what, and no way to head off potential data breaches.

To see this information, IT has to pull data from an operating system's many log sources such as the system audit journal and database journals, plus the history log and system operator message queue. Doing this manually takes more time than IT staff has to spare.

IBM i Log Sources

With the right tool to aggregate and query data, IBM i log sources can provide timely insights into the security of your data and systems. These sources, including journals and message queues recorded by the IBM i OS, create a comprehensive audit trail of changes. These critical log sources can be leveraged to monitor for security and compliance deviations, as well as to feed IBM i log data to Security and Information Event Management (SIEM) solutions that do not natively have visibility into the platform. It's important to note that by default you only have access to the history and system operations logs; you must configure logging for other log sources.

Making sense of the data written to many of these sources is nearly impossible. To stay compliant and monitor the security of IBM i systems, enterprises need a way to make sense of important events and quickly identify critical conditions without significant effort – or a major programming project.

System Audit Journal - QAUDJRN

The System Audit Journal (QAUDJRN) contains information related to events occurring on the IBM i system that impact security and can be used to log user and application activity. This includes information such as changes to system values, object authorities, profiles, authorization lists, object access attempts, and more.

The audit journal is read-only and cannot be overwritten, making it a perfect container to store system security information. However, the OS logs over 90 unique types of audit entries. It's challenging to write a custom program to pull significant events from the System Audit Journal, and nearly impossible to review audit data manually.

System Audit Journal - QAUDJRN

Operator messages are alerts that inform the operator about a condition that needs attention or about changes to the environment.

System and Application Messages – QSYSMSG Message Queue

QSYSMSG is an optional message queue that gives alerts about high priority system events. It should be created and monitored continuously.

QHST History Log

The QHST History Log is a message queue and a number of physical files that contain a list of messages that reflect certain events occurring on IBM i.

Assure Monitoring and Reporting

The Assure Monitoring and Reporting feature of Assure Security automates the analysis of data logged by IBM i systems to generate clear and actionable alerts and reports for various stakeholders – and optionally forward security log data to a SIEM.

Clear, Actionable Alerts and Reports

Assure Monitoring and Reporting is a powerful query engine with extensive reporting features. It automates the analysis of system and database activity found in IBM i log files to produce actionable alerts and clear, concise, easy-to-read reports.

Assure Monitoring and Reporting's purpose is to extract only pertinent data from journals so that administrators can focus on relevant information. No application modifications are required to leverage the benefits of Assure Monitoring and Reporting.

The feature is comprised of a System Module and a Database Module, which can operate independently or together. The System Module comprehensively monitors your system to report on changes to system objects, access attempts, powerful user activity, command line activity, access to sensitive data, and more. The Database Module alerts and reports on IBM i database activity.

The System Module also inspects static data sources such as QSYS.LIB, IFS objects, profiles, system values, authorization lists, jobs, spool files, and more to identify possible deviations from best practice.

The ability to easily monitor and report on static configuration settings, such as the public authority of objects, the current configuration of system values, or the values set for user profile parameters is essential given that analysis of these settings is a common step in a security audit.

Assure Monitoring and Reporting Core Features

As mentioned above, Assure Monitoring and Reporting is fundamentally a powerful filtering and query engine. The queries are created using a repository of field information that is generated based on the journals being monitored. As queries are run, they analyze journal entries and system information and extract the pertinent insights used to generate an alert or create a report.

To streamline implementation, predefined audit reports are provided for ERP applications such as Infor M3, and an out-of-the-box model is also provided for assessing GDPR compliance.

Reports can be run continuously, on a schedule or on-demand, and they can be formatted in PDF, XLS, CSV, or PF formats. PDF reports can be customized with specified logos, color schemes, and more, and reports can be distributed via SMTP (email), FTP, or the IFS.

With Assure Monitoring and Reporting, you can quickly produce reports on changes to system objects such as system values, user profiles, and authorization lists, as well as on data changes occurring outside an application or data changes to critical fields in your databases. You can also easily design custom reports on activities such as changes to sensitive database fields like bank account or credit card numbers.

Enabling Security Monitoring Across the Enterprise

While fairly uncommon just a few years ago, SIEM solutions are becoming integral to security strategies for many organizations. As the cost of data breaches continues to rise, organizations are finding it easier to justify the investment in SIEMs for early detection and fast response to threats.

SIEM technology aggregates data produced by security devices, network infrastructure, systems, and applications. That data is combined with contextual information about users, assets, threats, and vulnerabilities to enable real-time security monitoring, discovery of trends, incident investigation, and historical analysis.

Assure Monitoring and Reporting offers the ability to integrate IBM i log data into SIEM solutions such as IBM QRadar, Solar Winds, Splunk, ArcSight, LogRhythm, LogPoint, Netwrix and more for analysis alongside security data from other platforms. Leveraging its powerful query engine to extract log data from a number of sources, Assure Monitoring and Reporting's SIEM integration option securely builds and sends messages to a SIEM in message formats such as *LEEF, *CEF, *RFC3164, and *RFC5424.

Conclusion

IBM i journals and log files contain critical information regarding security-related activity occurring on your system. Continuous monitoring of this data is required to provide visibility into security events and compliance deviations. Unfortunately, this audit data is difficult to extract and understand in its native form.

Assure Monitoring and Reporting provides powerful query capabilities that automate analysis of IBM i journals, history files, and message queues to produce actionable alerts and clear, concise, easy-to-read reports on system activity, database changes, and static sources of information on your IBM i.

And, for organizations investing in SIEM solutions for security visibility across the enterprise, Assure Monitoring and Reporting's SIEM option integrates IBM i security information into the SIEM, enabling early detection and quick response to security incidents across all parts of the IT infrastructure.

precisely