Gain Greater Visibility into Your Epic Hyperspace Instance

Epic Systems Corp. is one of the largest providers of health information technology, used primarily by large U.S. hospitals and health systems to access, organize, store and share patient medical records. The Epic Electronic Health Record (EHR) system is widely recognized for its easy-to-use, fully integrated capabilities that cover clinical information, registration, patient scheduling, and billing.

With a solution that contains this much sensitive data and is subject to compliance mandates, it makes sense that you would want the maximum visibility possible to ensure data security.

Better Protect Patient Data

LogRhythm's Epic Hyperspace App provides a comprehensive solution focused on providing greater visibility into potential unusual activity within and related to Epic Systems Hyperspace EHR systems. This app provides you with:

- Real-time visibility (including alarms and reports) into:
  - Inappropriate access or access attempts to patient medical records
  - Inappropriate attempts to record or download patient medical records
  - Users and systems trying to access the EHR (appropriate and inappropriate)
- Context of the user who is accessing the patient records
- Logic or reasoning behind the attempted access to medical records

The LogRhythm Epic Hyperspace App makes it easy to get up and running quickly with pre-built content, such as AI Engine rules and alerts, dashboards, and reports.

How Does It Work?

The Epic App is available to LogRhythm platform customers through the LogRhythm Knowledge Base (KB). Updating the KB and enabling the app automatically creates the proper reports and AI Engine rules. Targeted Web Console dashboards can be downloaded from LogRhythm Community. Epic Hyperspace can then be configured to send Common Event Format (CEF) logs to the LogRhythm Platform.

LogRhythm offers full log parsing support for 30+ events forwarded from Epic. Log parsing forms the foundation for more advanced integrations such as dashboards, AI Engine correlation/trending rules, and reports.

Unlike other SIEM solutions that simply ingest syslog from Epic, the LogRhythm Platform delivers:

- Data normalization and classification
- AI Engine correlation rules for suspicious activity specific to Epic
- Web console dashboards for real-time monitoring of activity in Epic
- Reporting for roll-ups of user activity within Epic
- Enhanced data enrichment via LogRhythm's MDI Fabric

LogRhythm's Epic Hyperspace App

Benefits

- Greater visibility and real-time awareness into user activity in Epic Hyperspace EHR software to better protect patient medical records and other sensitive data

- Simplify your security monitoring and quickly surface the most critical events with Epic-specific dashboards

- Pre-built content for Epic Hyperspace means your team can focus their attention on mission-critical tasks, not setting up integrations

Epic Hyperspace App and Health Care Compliance

The LogRhythm Epic Hyperspace App complements our Health Care Compliance Automation Module to help your organization comply with HIPAA, HITECH, and Meaningful Use guidelines.

The LogRhythm Epic Hyperspace App in Action

Use Case: Monitoring for VPN-Based Access

Many organizations do not allow remote access of patient records, due to data leak and privacy concerns. When paired with LogRhythm's geolocation capabilities, the LogRhythm Epic Hyperspace App provides monitoring for VPN-based access to Epic to quickly alert on remote security threats. Whether it's an employee with good intentions or a malicious attacker, your security team can act on these incidents (e.g., automatically locking down the user account using SmartResponse™ to prevent data exfiltration).

Use Case: Employee Snooping

Employees may try accessing records that they shouldn't (e.g., viewing records for a high-profile patient or accessing an excessive number of records). The LogRhythm Epic Hyperspace App provides monitoring for excessive Break-the-Glass Access (i.e., a quick means for a person who does not have access privileges to certain information to gain access when necessary), both by user and by patient. Built-in rules trend access by user and by patient. When there is an anomalous number of access attempts, an alarm will fire. Your team can then launch a response, including locking down the endpoint or blocking the user's access.

Use Case: Account Takeover Detection with User and Entity Behavior Analytics (UEBA)

Quickly and accurately detecting an account that's been compromised is critical to ensuring minimal damage. The visibility provided by the LogRhythm Epic Hyperspace App can rapidly surface and alert on indicators of compromise. For example, if the LogRhythm Platform detects an Epic user password was changed, followed by an unusual number of attempts to access a user's Epic account, the LogRhythm Platform will fire an alarm to notify your security team to take immediate action.
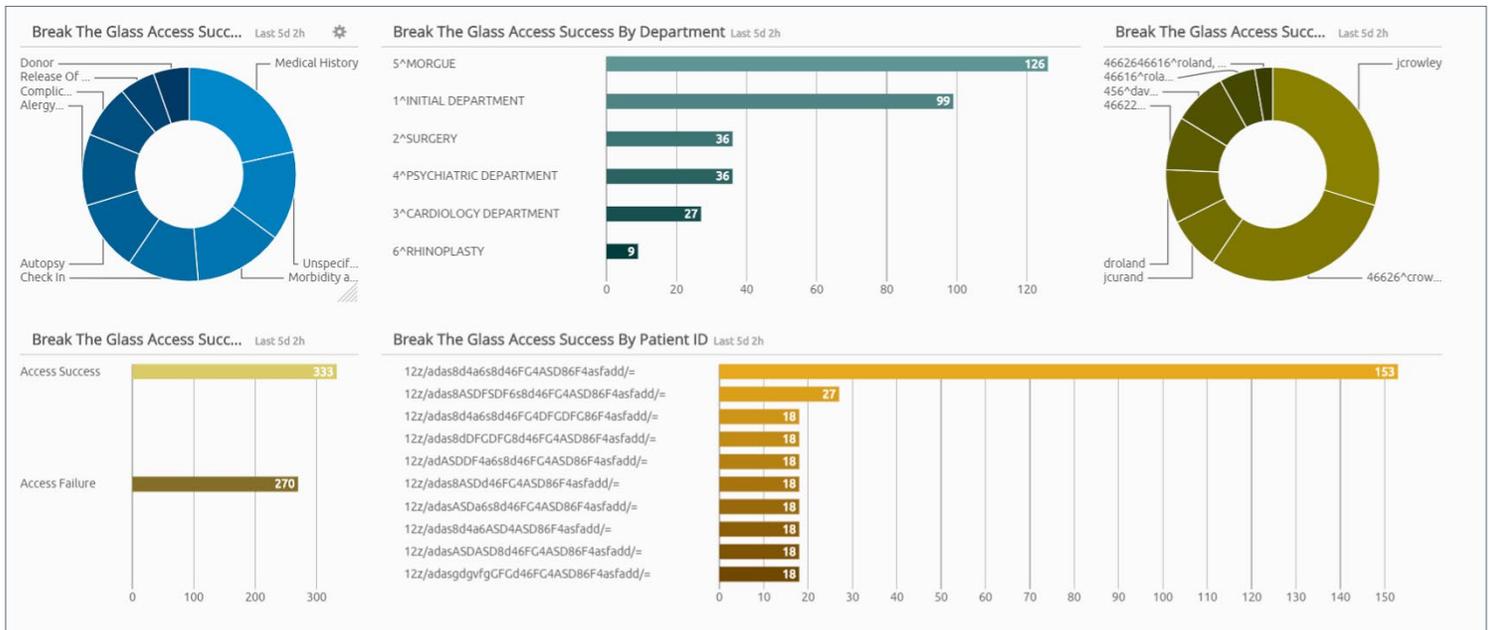
Successful Break-the-Glass Dashboard

Additional Reading:

• Guides: Epic Hyperspace App resources on LogRhythm Community

• White Paper: Health Care Compliance Made Easy: The LogRhythm Health Care Compliance Automation Module