PRODUCT OVERVIEW

LogRhythm and FairWarning®: Cyber Security for Healthcare

LogRhythm
The Security Intelligence Company

LogRhythm and FairWarning, Inc. have developed an integrated solution for comprehensive privacy auditing and monitoring capabilities. It delivers immediate protection from cyber security threats and data breaches such as unlawful access to Protected Health Information (PHI), and ensures compliance with regulatory mandates such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Healthcare organizations benefit from comprehensive security monitoring for more than 170 healthcare applications, with automated detection and alerting on suspicious activity and policy violations, including inappropriate user access to patient healthcare information.

With LogRhythm and FairWarning®, healthcare organizations now have the means to monitor and secure the entire range of systems and applications across their organizations and perform comprehensive forensic investigations of suspected breaches.

LogRhythm for Healthcare

- ☑ Out-of-the-box HIPAA/HITECH Support
- ☑ Easy-to-Install, Use, and Manage
- ☑ Flexible Deployment Options
- ☑ Rapid, Powerful Forensics
- ☑ Real-time Advanced Correlation

LogRhythm

LogRhythm empowers organizations to detect, respond to and neutralize cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. LogRhythm solutions also deliver rapid compliance automation and assurance, and enhanced IT intelligence.

LogRhythm's award-winning Security Intelligence Platform integrates next-gen SIEM and log management with network forensics, endpoint monitoring and multidimensional security analytics. Its collaborative incident response orchestration and patented Smart**Response** automation framework help security teams perform end-to-end threat lifecycle management. LogRhythm's unified solution powers the next-gen SOC, accelerating the detection and response to emergent threats across the holistic attack surface.

FairWarning®

FairWarning® delivers privacy auditing solutions that are essential for compliance with healthcare privacy regulations such as ARRA HITECH privacy and Meaningful Use criteria, HIPAA, and other regulatory responsibilities. It also minimizes the risks, burdens and costs associated with a major patient privacy breach by automating inefficient manual processes. Detecting and preventing privacy breaches helps mitigate the risk of patient lawsuits and unwanted media attention. FairWarning® also addresses best practices for:

- California S.B. 541 and A.B. 211 (2009 anti-snooping legislation for healthcare)
- Canadian provincial law such as Alberta's Health Information Act of 2010
- EU Data Protection Directive
- France Health Information Systems Security Directive (ASIP schedule 2010)
- France Patient Rights Law of 2002
- NEN 75-10 and NEN 75-13 (Netherlands)
- Texas H.B. 300
- U.K. Caldicott Guardian Act (United Kingdom)

LogRhythm and FairWarning® in Action

LogRhythm and FairWarning® are tightly integrated to bridge the gap between highly proprietary Electronic Health Record (EHR) system auditing and security operations, delivering the tools that healthcare organizations need to control access to confidential data and to respond appropriately when policy is violated.

Controlling Access to PHI

Challenge Healthcare organizations require open access to confidential data in the case of an emergency, making it difficult to identify or control unauthorized access to protected health information (PHI). This challenge is compounded by an inability to correlate EHR-related activity to corresponding user behavior.

Solution LogRhythm receives automatic notification of policy violations and potential patient record breaches directly from FairWarning®. Alarms can be immediately analyzed against any other relevant context surrounding the event to quickly identify the who, what, when, and where of a patient data breach.

Benefit Event data from FairWarning® can be easily customized to hide patient data, delivering relevant event detail to LogRhythm without exposing confidential data. This allows security administrators to respond quickly and accurately to an incident without exposing PHI to unauthorized viewers.

Breach Notification

Challenge Organizations that experience a PHI data breach are required to report the incident with all relevant details about the incident in a timely fashion. Without the ability to tie specific EHR-related activity with accurate forensic data, organizations risk exposure to hefty fines and additional risks.

Solution FairWarning® audits all access to patient records within EHR applications, including potential breaches such as a high-profile patient record being improperly accessed. Wizard-driven investigation and reporting tools within LogRhythm make it easy to access the detail surrounding any potential breach for accurate, rapid reporting.

Benefit Security administrators and auditors have access to incident-related information in out-of-the-box formats, allowing them to expedite the breach reporting process. A digital chain of custody provides tamper-proof evidence for subsequent investigations and inquiries.

FAIRWARNING.

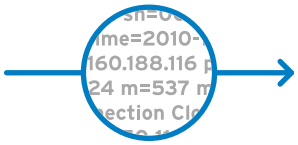
LogRhythm®

Electronic Health Records

- Epic
- McKesson
- GE
- Meditech
- Siemens
- Allscripts
- Etc.

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data



Machine Data Intelligence

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically take action and respond to events and alarms

Security Intelligence Platform

- Next Generation Security Operations Center
- Security Analytics
- SIEM & Log Management
- Network Monitoring and Forensics
- Endpoint Monitoring and Forensics
- Behavioral Analytics (e.g. UBA, NBAD, EDR)

LogRhythm Labs