FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Compliance and Integrity Monitoring for EMR Systems

The value of electronic medical record (EMR) systems is immense. These digital records are designed to be available anytime and anywhere, connecting healthcare providers with patient data. EMRs are a central repository of patient medical histories, medications, diagnoses, immunization dates, allergies, lab results and radiology images. With this accurate and up-to-date patient information, providers can offer optimal care, automate the provider's workflow, support changes in payer requirements and address patient needs.

> *Tripwire offers unique monitoring for Epic systems. Tripwire's automated monitoring of our Epic system allowed us to achieve our first passing audit while minimizing a hacker's attempt to compromise the data.*
>
> **—Major US Hospital**

Given the sensitive information EMRs contain, the need for privacy and security is a high priority. This is reflected in the U.S. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules, which state the need to protect privacy and security of individually identifiable health information found on EMRs. The HIPAA Privacy Rule covers protected health information (PHI) in any medium, while the HIPAA Security Rule covers electronic protected health information (ePHI). Healthcare is the third-most common industry being breached by hackers, just behind financial services and professional services (Verizon 2022 Data Breach Investigations Report).

Protect Your EMR System

Continuous monitoring of system level configuration and data integrity is a foundational control to mitigate cyberattacks on EMR systems. This provides your organization with visibility into unauthorized or unexpected changes that may be the result of errors, omissions or—worse—malicious activity. Some EMR environments can have up to ten million changes in one month. Monitoring complex environments like these can be easier said than done, especially when monitoring affects performance or cannot be done natively due to the system architecture. Some providers monitor the database by creating scripts and running them against the database in a scheduled manner. However, scripts are inadequate because they only offer a point in time snapshot rather than continuous monitoring.

Other providers might use specialized tools for monitoring the EMR environment. However, such tools often don't provide this information in the context of the security posture of your entire environment. Thus, security teams in healthcare organizations lack the end-to-end visibility of the security posture of their entire environment.

EMR Integrity Monitoring from Tripwire

Fortra's Tripwire delivers the necessary foundational controls to help healthcare providers protect patient data residing on Electronic Medical Record systems from unauthorized changes and prove compliance. We ensure the security of PHI on EMR systems by leveraging the controls to provide:

- Out-of-the-box monitoring for critical file change on EMR systems
- Secure configuration compliance for multiple standards like HIPAA, NIST 800 (53 & 171), PCI and many others with a single solution for the entire EMR environment
- Automation with business systems: CMDB, Service Desk, and SIEM tools. (e.g. QRadar, Splunk, ServiceNow) to provide end-to-end visibility

Tripwire EMR Monitoring Features

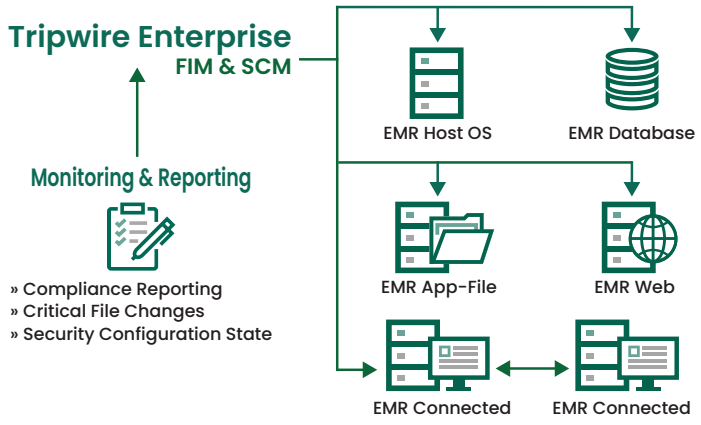
Out-of-the-box monitoring for security configuration compliance—Ensure compliance with HIPAA, NIST 800-(53 & 171), PCI and other regulatory standards across the entire EMR environment. Configuration assessment with file integrity monitoring to detect, analyze and report on changes as they happen and keep configurations continually compliant. This immediate access to change information lets you fix issues before they result in a major data breach, audit finding or long-term outage.

Support for maintaining a secure state across EMR systems and critical assets—Out-of-the-box monitoring for critical file changes on:

- Application Delivery Platform & Business Continuity Systems (e.g. Citrix, Red Hat, Windows, HP-UX and AIX)
- AD/LDAP (Active Directory and User & Role Management software)
- Databases (MSSQL, Oracle, Caché via Chronicles master files)
- In-scope network devices
- Virtual environments (e.g. Citrix, Hyper-V, VMware)

Faster, easier audit preparation—Dramatically reduce the time and effort for audit preparation by obtaining continuous, comprehensive IT infrastructure baselines, along with real-time change detection and built-in intelligence to determine the impact of change.

Automation with business systems: CMDB, Service Desk, Enhanced SIEM—Maximized automation capabilities for security and event alerting practices, change management process integrations and audit prep activities.



Tripwire provides FIM and SCM capabilities to EMR systems and monitoring and reporting of results.

Summary

Tripwire's integrity monitoring and secure configuration management solutions are foundational security controls that allow healthcare organizations to achieve and maintain compliance while gaining operational efficiencies in managing their Epic, Cerner and Allscripts infrastructure. Healthcare providers can use Tripwire for assurance that their EMR systems are secure through integrity solutions that minimize the risk of malicious attacks, fraudulent activity and unauthorized changes, and deliver exceptional system availability and security.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.