SOLUTION BRIEF

Maintaining the Security and Integrity of EHR Systems

The Tripwire EHR Solution

Highlights

- Simple subscription pricing for best-in-class FIM and SCM
- Detailed understanding of good vs. bad changes
- Broadest depth and breadth of compliance policy and platform coverage
- Tailored advice, incident assistance and audit support related to Tripwire findings
- Cloud-hosted infrastructure combined with consulting services

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

Beyond those benefits, by using EHRs providers can access and consult with data sets related to the patient's diagnosis and implement best care practices. On the compliance front, EHRs are intended to meet "meaningful use" standards to measure improved health care quality and efficiency. These metrics are focused on patient-centered, evidence-based, and prevention-oriented efficiency. In the United States, eligible hospitals and critical care providers have been given financial incentives to move to EHRs. The Office of the National Coordinator (ONC) can also certify EHR providers as "meaningful use" with the Health IT Certification Program (a voluntary certification program). Some common EHR systems used are Epic, Cerner, and Allscripts. Epic is used by many large hospital systems, making it one of the top three EHR systems in the US. It is also ONC 2015 Certified, so Epic users can meet federal mandates.

EHR: Prime Targets for Cyber Attacks

Given the sensitive information EHRs contain, the need for privacy and

security is a high priority. This is reflected in the US 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 EHRs. 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 second-most common industry being targeted by hackers, just behind financial services (Verizon 2017 Data Breach Investigations Report).

For healthcare organizations, the average cost of a stolen patient record is $355, compared with $5–$30 for financial data. In other words, PHI is a more valuable cybercrime opportunity. By taking advantage of patients' medical conditions or claim settlements, criminals can use PHI to target their victims with frauds and scams. Attackers can also create fake insurance claims, allowing for the purchase and resale of medical equipment. Or they can use PHI to illegally gain access to prescriptions for their own use or resale. If they have access to a real-time database, they can change the payment directions to redirect funds. The range of attacker motives and methods in healthcare is daunting—and increasing.

Defend and Protect Your EHR

Continuous monitoring of system level configurations and data integrity are foundational controls for mitigating cyberattacks on EHR systems. They provide organizations with visibility into unauthorized or unexpected changes that may be the result of errors, omissions or—worse—malicious activity. Some EHR 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. This resultant monitoring gap—between two instances of when the script has been run—presents a security challenge as it provides a window of opportunity to attackers. As a result, the script approach is often unacceptable to auditors.

Even in situations where the EHR system has native functionality for monitoring unauthorized access, using these features can be time consuming and cumbersome, and can quickly overwhelm an IT operations department.

The Tripwire EHR Solution

Tripwire's EHR solution provides a tailored package of products and expertise to alleviate the challenges of monitoring EHR systems for unauthorized changes and to ensure that those systems are in compliance with HIPAA and NIST 800-53 & 171. The solution leverages Tripwire® Enterprise, a proven security configuration management (SCM) and file integrity monitoring (FIM) solution. Tripwire Enterprise provides healthcare organizations using Epic, Cerner or Allscripts EHR systems out-of-the-box monitoring for critical file change, security configuration compliance with HIPAA, NIST 800-53 & 171, and PCI 3.2, as well as reports that provide audit-ready evidence of compliance with security controls. Tripwire Enterprise provides this coverage across the entire EHR environment, including:

- 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)
- Database (MSSQL, Oracle, Caché (via Chronicles master files))
- In-scope network devices
- Virtual Environment (e.g. Citrix, Hyper-V, VMware)

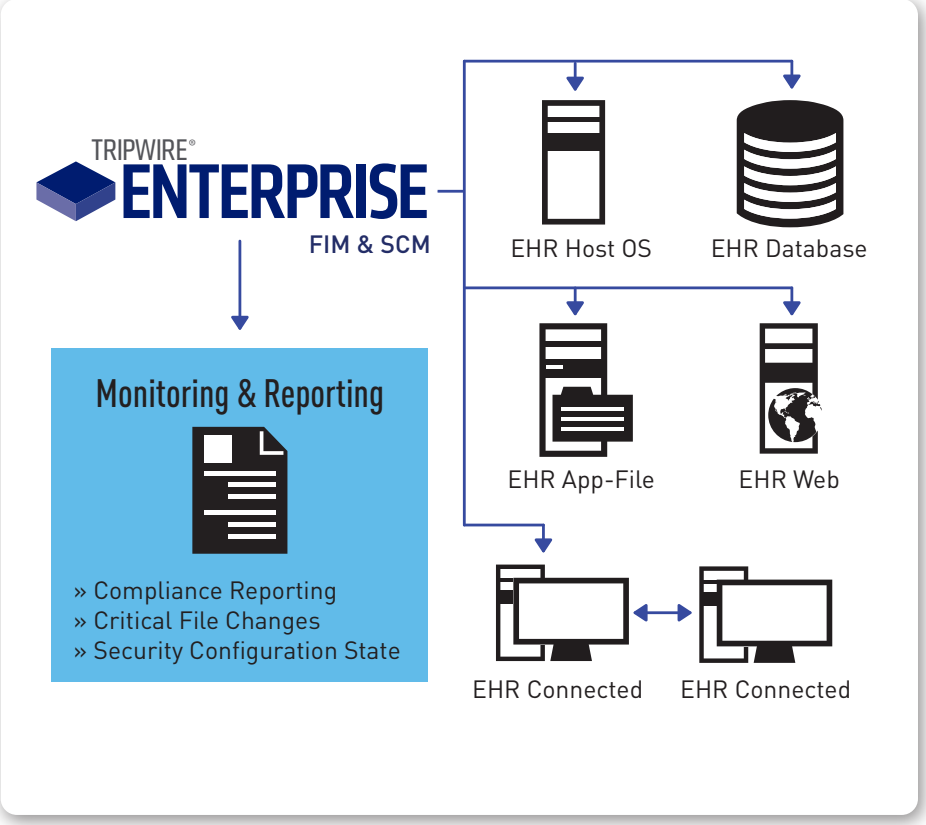

Fig 1 The Tripwire EHR Solution provides FIM and SCM capabilities to EHR systems and monitoring and reporting of results.

To ensure effective tailoring and deployment of Tripwire products to the specific EHR system, Tripwire's EHR solution provides consulting from Tripwire Professional Services. These experienced consultants work with healthcare organizations to create targeted rules for monitoring the EHR application and EHR database content, as well as hardening policies. The Tripwire EHR Solution also provides enhanced automation through integrations with change management practices, ITSM and analytics tools (e.g. Splunk, QRadar and ServiceNow).

Tripwire Enterprise's file integrity monitoring and secure configuration management capabilities are foundational security controls that allow healthcare organizations to achieve and maintain compliance while gaining operational efficiencies in managing their Epic, Cerner or Allscripts infrastructure. By minimizing the risk of malicious attacks, fraudulent activity and unauthorized changes, and by gaining exceptional system availability, healthcare providers can depend on Tripwire's integrity assurance solutions for robust EHR security.

> 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

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

SBEHRS2a 2102