SOLUTION BRIEF

Tripwire Cybersecurity and Compliance for Healthcare Organizations

Quote

"Almost half of patients said they'd find a different healthcare provider if informed their medical records were stolen. Given the lifetime economic value of a patient, providers are at risk of losing $305 billion in cumulative lifetime patient revenue over the next five years due to medical identity theft."

The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider CyberSecurity In action

—Accenture, 2015

In May 2015, Ponemon Institute and ID Experts conducted a benchmark that found that, for the first time, criminal attacks are primary cause of healthcare data breaches. This is a 125 percent increase over the past five years. Why? Because healthcare organizations and their business partners obtain and share highly valuable patient data. And, taken as a whole, the healthcare industry provides a large (and growing) attack surface for criminals who are eager to exploit this information.

Patient records have most everything the attacker needs in a single record to carry out sophisticated insurance fraud schemes, purchase medical supplies or drugs, or commit other types of fraud including outright identity theft. Recent studies have determined that cyber criminals can sell the comprehensive identity information found in a health insurance or patient record for as much as $1,000 on the black market. Compare that to the average cost of a stolen credit card that fetches about $1 on the black market, and you can see why healthcare organizations are so frequently targeted.

The deployment of new devices—especially those categorized as IoT that use wireless networks and sensors to collect and exchange information—is a double-edged sword. While these devices offer medical environments tremendous capabilities to care for patients and increase efficiencies, each device increases an organization's attack surface.

Adding to the complexity of these security challenges are compliance and regulatory frameworks (such as HIPAA, NIST, ISO, PCI and COBIT) typically enacted to protect systems and sensitive data. However, since they frequently evolve to keep pace with information technology, industry influences and new threats to systems and data, healthcare organizations face multiple moving targets for managing controls and meeting requirements.

All this said, securing patient, customer and organizational data must be a top priority. The high price for patient records, combined with new and growing vulnerabilities, provide a great impetus for cybercriminals to attack.

How to Keep Your Healthcare Organization Safe

There are several key measures to follow that help lower the risks of breaches and keep your company's and customers' data safe.

- Build a risk-aware culture. This means:
  - Thoroughly examine and determine where in your organizations security risks lie
  - Educate and communicate with employees to help them understand how they can help close the gaps
  - Implement the right tools that continuously monitor and identify vulnerabilities and alert employees so that your organization can act quickly to reduce the risks.
- Implement foundational controls and basic security hygiene.
  - According to SANS, implementing the first six CIS Controls provides a highly effective and efficient level of defense against the majority of real-world attacks, and provides the necessary foundation for dealing with more advanced attacks
- Automate all security and compliance efforts. This helps to:
  - Discover and profile all business critical assets, such as patient care systems, medical devices, and payment systems.
  - Quickly repair configurations errors
  - Adjust security controls based on system changes and business impact
  - Monitor, measure and report compliance with security and privacy requirements.
- Manage incidents with intelligence to help your organization to respond more quickly. To do this:
  - Implement intelligent analytics to help monitor operations
  - Implement automated response capabilities
  - Integrate next generation threat intelligence solutions with change detection for advanced threat detection and response

Tripwire's Proactive, Continuous Monitoring Approach

Tripwire has a significant history helping security and IT professionals in the healthcare industry harden systems and identify change and vulnerabilities.

- Tripwire is the trusted endpoint monitoring solution for business critical systems, delivering a best in class solution built on a foundation of innovation and deep security expertise. Over 9,000 organizations use Tripwire across a broad platform on over one million business critical endpoints.
- Tripwire delivers 10 of the CIS Controls—with virtually complete coverage of the first six—which provides 80% of your security hygiene
- Tripwire offers an open architecture with APIs and frameworks, such as STIX, TAXII and CybOX, so you can quickly leverage intelligence from a variety of sources to proactively alert to new threats as they occur

Table 1. First Six CIS Controls: High Impact, Immediate Benefits

Category	Control Title(s)	Why It's so Important
Know What You Are Protecting	CIS Control #1: Inventory of Authorized and Unauthorized Devices CIS Control #2: Inventory of Authorized and Unauthorized Software	The first two Controls require rigor in knowing what endpoints must be protected and what software is running on those endpoints. Although many IT organizations have some version of a Configuration Management Database, invariably security teams find devices and software that are either not visible to or not managed by IT operations.
Define Secure Configuration Baselines	CIS Control #3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	With an accurate inventory in place, the next step is evaluating the configuration of endpoints against configuration standards, such as the CIS benchmarks, the United States Department of Defense (DoD) Security Technical Implementation Guide (STIG) and so forth.
Continuously Monitor Vulnerability of Resources	CIS Control #4: Continuous Vulnerability Assessment and Remediation	After the baseline is known and endpoints are configured securely, those configurations must be monitored for changes that introduce vulnerabilities or the availability of patches or upgrades needed to maintain security.
Limit and Monitor Administrative Privileges	CIS Control #5: Controlled Use of Administrative Privileges	Having addressed the basic vulnerabilities of the hardware and software resources, the vulnerabilities of user accounts must be minimized. Maintaining the least privilege to support "need to share" while maintaining "need to know" can keep malicious software from successfully executing if it does get installed.
Continuous Monitoring/Situational Awareness	CIS Control #6: Maintenance, Monitoring, and Analysis of Audit Logs	Nothing stands still: IT installs new software, threats develop new attacks, organizations and priorities change. Situational awareness is key for security teams to focus on deploying resources in the most effective and efficient areas to meet business security needs.

Table 1 The importance of the first six CIS Controls, based on SANS research.

» Tripwire delivers high-fidelity detection with real-time, continuous monitoring and correlation capabilities to detect changes that can potentially be a targeted attack

» Finally, Tripwire has a single multi-service, highly resilient agent for advanced detection and monitoring to preempt cyber attacks. It is more reliable, trusted, stable, accurate and faster than any other method for monitoring thousands of critical servers

Advanced Cybersecurity for Today's Threats

The solution to the unprecedented cyberthreat problem that healthcare organizations face is to implement foundational controls that integrate into other solutions to proactively respond to threats. Tripwire delivers foundational controls (including file integrity monitoring, configuration management, asset discovery, and vulnerability and log management) to strengthen your security and compliance posture. Our solutions are based on high-fidelity asset visibility and deep endpoint intelligence, combined with business context. Together, these solutions automate and integrate security and IT operations. Each solution has core capabilities in different areas in the information security space. They help solve your most complex security and compliance challenges, and help you make better, more informed decisions. Tripwire even offers unique monitoring and support for electronic healthcare record (EHR) systems.

A Larger Attack Surface Equals More Exploits

When SANS Institute examined intelligence data specific to the healthcare sector it found alarming evidence that supports the claim made in a study by the Ponemon Institute: 94 percent of medical institutions said their organizations have been victims of a cyber attack. The SANS analysis "not only confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen."

The biggest culprits, says SANS, are IoT (Internet of Things) devices – from connected medical devices to conferencing systems to edge security technologies. According to the findings, it was startling to discover that "some of these devices and applications were openly exploitable (such as default admin passwords) for many months before the breached organization recognized or repaired the breach," evidence that many organizations were out of compliance.

Ultimately, advice from SANS to healthcare organizations is to enforce best practices and controls, including:

» Know the hardware and software on your network

» Be aware of the many attack surfaces and determine their current state

» Secure devices by following industry and manufacturer/vendor best practices

» Continually monitor them for unauthorized change or access

To read the full SANS Institute report, "*Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*," visit: sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

Key benefits of Tripwire solutions include:

» An integrated approach to threat protection based on consolidated vulnerability and change intelligence that dramatically accelerates threat detection and prioritization. This allows customers to detect cyberthreats sooner by identifying network "hot spots" indicative of an attack—places where risk is high and suspicious changes are occurring.

» Continuous attack surface analysis that makes it possible for users to rapidly and proactively identify the most critical security issues using business impact and visual vulnerability risk matrix scoring.

- Tripwire® IP360™ facilitates this analysis by enabling customers to discover every device, software and application for a comprehensive view of the network. The solution uses advanced analytics and a unique quantitative scoring algorithm based on several factors—including the vulnerability score and business-relevant asset value—to prioritize the vulnerabilities for remediation. The result is actionable data that enables IT security teams to focus on the tasks that will quickly and effectively reduce overall network risk with the fewest possible resources.

» Significant reduction of enterprise security risks through rapid identification and response to specific

vulnerabilities and malware (like ShellShock and Heartbleed) from a continually updated library of over 100,000 conditions, including vulnerabilities, configurations and operating systems, and more than 15,000 applications.

» Improves operational efficiency by prioritizing remediation efforts on the greatest risks.

» When it comes to compliance, Tripwire Enterprise offers more than 800 policies for almost any platform or device, and for the multiple compliance mandates faced by organizations. Organizations can assess configurations to learn where they fall short of compliance, get guidance to fix issues, and establish and maintain configurations in a compliant and secure state. It then determines when changes occur to that compliant and secure state and assesses them to determine if they introduce non-compliance or security issues. When Tripwire Enterprise finds an undesirable change it offers remediation advice to return systems to a compliant state. Tripwire Enterprise monitors EPIC systems for change on critical data on the EHR system while avoiding flooding the process with distracting, unhelpful change information.

> "Tripwire's automated discovery and granular risk scoring enabled us to prioritize remediation around threats faster. Tripwires's scaling was critical since we have a wide geographic coverage."
>
> —Large healthcare insurance provider

» Eliminates extensive manual work, saving time and resources, by automating common responses.

» Additionally, Tripwire solutions integrate with a number of other security solutions for analytics, forensics, SIEM and threat response. With these integrations, they deliver actionable reports and alerts and enable the integration of valuable endpoint intelligence into operational systems like change management databases, ticketing systems, patch management and security solutions.

- Tripwire Log Center® integrates data from Tripwire Enterprise and Tripwire IP360, which provides organizations with insight into the relationships between suspicious events, system changes, weak configurations and current vulnerabilities. It reduces the workload and costs associated with traditional SIEMs and security analytics solutions by pre-filtering data and identifying anomalies and patterns known to be threats and early indicators of breaches. This allows Tripwire Log Center to forward only actionable, relevant data to SOC staff and third-party tools (such as threat intelligence solutions).

Good Security Delivers Effective Compliance

If an organization has implemented good security processes and controls, they could be well on their way to meeting multiple compliance and/or security standards. Tripwire supports many compliance mandates (including HIPAA and FDA), and guidelines from NIST. That support, combined with Tripwire's advanced cybersecurity and compliance solutions, you get proven, industry-recognized security and the ability to meet almost any compliance mandate. All while helping you detect and respond to any threat to your organization's—and customers'—data.

What Next?

To learn more about Tripwire's solutions for healthcare organizations, visit **tripwire.com/solutions/solutions-by-industry/healthcare** or request a demo at **tripwire.com/contact/request-demo**

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

SBHS3a 2102