AnchorPoint Security

Integrated Threat Response

The Perfect Rx for HIPAA Compliance

Meeting and demonstrating compliance with HIPAA requirements presents a number of operational challenges for covered entities, whose ultimate goal is patient care. So when it comes to protecting the ePHI of those patients, and demonstrating that security controls are in place and working, it's critical to do this as quickly, efficiently and accurately as possible. That way, the organization can focus on what matters.

Unlike traditional SIEM solutions, AnchorPoint's Integrated Threat Response (ITR) service delivers all of the core security capabilities you need to be ready for your audit—from day one. There is no need for purchasing, deploying, and integrating asset discovery, threat detection, vulnerability assessment, network analysis and reporting tools. We've built in the core security capabilities to save you the time, cost, and complexity of purchasing, configuring, and integrating those disparate data feeds and managing disparate management consoles. All you need to be ready for your audit is "instantly on" when we start monitoring.

Additionally, AnchorPoint's security intelligence capability is backed by global threat research collected and analyzed by our Security Operations Center (SOC). We integrate threat intelligence feeds from industry leaders and the open source community to stay ahead of threats to your business.

HIPAA Requirement		Relevant AnchorPoint ITR Capabilities	Benefits of Integrated Threat Response
§164.308 Risk Analysis	Conduct an accurate assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.	• Asset Discovery • Vulnerability Assessment • Network Intrusion Detection (NIDS) • Host-based Intrusion Detection (HIDS) • Wireless IDS • File Integrity Monitoring • SIEM • Risk Scoring & Analysis	• Included asset discovery, vulnerability assessment, threat detection, behavioral monitoring, and security intelligence - ***provides a complete picture of your risk posture, within hours of deployment*** • Accurate and consolidated asset inventories combined with real-time vulnerability assessment data is essential for auditor reviews and assessments. • Accelerated audit procedures because integration is already completed—as soon as AnchorPoint Security starts monitoring.
§164.308 Information System Activity Review	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	• Vulnerability Assessment • Network Intrusion Detection (NIDS) • Host-based Intrusion Detection (HIDS) • Wireless IDS • File Integrity Monitoring • SIEM • Behavioral Monitoring • Log Management	• Included asset discovery, vulnerability assessment, thread detection, behavior monitoring, and security intelligence - ***reduces the cost and complexity of compliance.*** • Integrated log review and analysis, with triggered alerts for high risk systems (containing ePHI). • Customized, action-oriented alerts which tell you exactly what to do, rather than add to the noise. • Integrated threat data backed by AnchorPoint's Security Operations Center (SOC).
§164.308 Access Authorization, Establishment and Modification	Implement policies and procedures that grant, establish, document, review and modify a user's access to assets.	• Asset Discovery • Host-based Intrusion Detection (HIDS) • File Integrity Monitoring • SIEM	• Automatically discover all ePHI assets via included asset discover - no costly and complicated integration required. • Monitor changes to critical files with included file integrity monitoring.

Integrated Threat Response for HIPAA Compliance

HIPAA Requirement		Relevant AnchorPoint ITR Capabilities	Benefits of Integrated Threat Response
§164.308 Log-in Monitoring	Procedures for monitoring log-in attempts and reporting discrepancies.	• Host-based Intrusion Detection (HIDS) • SIEM	• Included HIDS monitors all activity on critical files and systems • Included SIEM correlates events that could signal policy violations such as unauthorized logins followed by additional security exposures such as data exfiltration. • Custom dashboards and reports facilitate audit reviews.
§164.308 Protection from Malicious Software	Procedures for guarding against, detecting, and reporting malicious software.	• Vulnerability Assessment • Network Intrusion Detection (NIDS) • Host-based Intrusion Detection (HIDS) • Wireless IDS • File Integrity Monitoring • SIEM • Behavioral Monitoring	• Included vulnerability assessment discovers hosts and applications that may be vulnerable to malware and other exploits. • Included threat detection (NIDS, HIDS, and Wireless IDS) detects and alerts on potential infections and exposures. • Included file integrity monitoring alerts on changes to critical files which could signal malicious intent or malware infection. • Integrated core security delivers the security intelligence required to respond to and contain malware outbreaks.
§164.308 Password Management	Procedures for creating, changing, and safeguarding passwords.	• Vulnerability Assessment • Host-based Intrusion Detection (HIDS) • File Integrity Monitoring • SIEM	• Included vulnerability assessment identifies the use of weak and default passwords. • Included host based intrusion detection and file integrity monitoring will signal when password files and other critical system files have been modified. • Integrated security intelligence connects critical, yet related events across systems such as a password change followed by exfiltration of data from the same device.
§164.308 Security Incident Response and Reporting	Identify and respond to suspected or known security incidents; mitigate harmful effects of known security incidents and document security incidents and their outcomes.	• Vulnerability Assessment • Network Intrusion Detection (NIDS) • Host-based Intrusion Detection (HIDS) • Wireless IDS • File Integrity Monitoring • SIEM • Behavioral Monitoring • Log Management • Situational Awareness	• included asset discovery, vulnerability assessment, threat detection, behavioral monitoring, and security intelligence - accelerates the incident response process. • Integrated log review and analysis, with triggered alerts for high risk systems (containing ePHI). • Customized, action-oriented alerts which tell you exactly what to do next when responding to incidents. • Integrated threat data backed by AnchorPoint's Security Operations Center (SOC).
§164.310 Device and Media Controls	Implement policies and procedures that govern the recipe and removal of hardware and electronic media that contain ePHI.	• Host-based Intrusion Detection (HIDS) • File Integrity Monitoring • SIEM	• included HIDS will alert on policy violations such as attempted use of external storage media on critical systems (e.g USB drives). • included file integrity monitoring captures anomalous changes to critical files containing ePHI. • Event correlation rules provide the situational awareness needed to identify the potential exfiltration of ePHI.

Integrated Threat Response for HIPAA Compliance

HIPAA Requirement		Relevant AnchorPoint ITR Capabilities	Benefits of Integrated Threat Response
§164.312 Encryption and Decryption	Implement a mechanism to encrypt and decrypt ePHI.	• Asset Discovery • Behavioral Monitoring • Host-based Intrusion Detection (HIDS) • Network Intrusion Detection (NIDS) • Wireless IDS	• Automatically discover all ePHI assets via included asset discovery - no costly and complicated integration required. • AnchorPoint will detect and alert when encryption or decryption procedures are not implemented correctly.

Summary

Traditional SIEM approaches aren't sufficient for today's cyber security landscape and changing compliance requirements. They're costly, complex, and they take too long to deploy. AnchorPoint Integrated Threat Response delivers more functionality—at reduced costs—and in significantly less time. Accelerated audits are just what the doctor ordered.

AnchorPoint's mission is to bring enterprise-class information security to the under served small to mid-size market. AnchorPoint Security is a privately held company headquartered in Oklahoma City with 10 employees and an advisory board with over 40 years of combined experience in information security and risk management in highly regulated industries.

For more information on how AnchorPoint Security can help you meet your HIPAA compliance needs, contact us at +1-800-731-1963 or send email to sales@anchorpointsec.com.

AnchorPoint Security