ALERT LOGIC®

SOLUTION OVERVIEW:

ALERT LOGIC® FOR HIPAA COMPLIANCE

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

Alert Logic provides organizations with the most advanced and cost-effective means to secure their healthcare networks and help them achieve compliance with HIPAA, HITECH and Meaningful Use mandates. As Meaningful Use is driving greater use of electronic health records (EHR) within the healthcare industry and making protected health information (PHI) more easily accessible to medical professionals, it is also creating opportunities for identity theft and medical claim fraud. Medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 20131. Healthcare organizations are exposed to a higher risk of breach than other industries for two reasons: (a) PHI is significantly more valuable on the black market than other personally identifiable information such as credit card data, and (b) healthcare security systems are typically lagging other sectors, as evidenced by the FBI 2014 Private Industry Notification (PIN)3.

The Health Insurance Portability and Accountability Act (HIPAA) outlines several administrative, physical and technical safeguards for covered entities and business associates in healthcare. Together these safeguards create a proactive approach to discovering and addressing vulnerabilities and suspicious network activity, thereby reducing risk for these organizations. Also, with the passage of the Omnibus Act of 2013 and HITECH Act of 2009, cleaning up after a breach will usually be more expensive and damaging than preventing one, making compliance with HIPAA all that much more important.

"Alert Logic solutions are a critical component in our overall security strategy for Methodist Health System. Protecting patient data is our number one priority and Alert Logic helps us do just that."

-Wayne Keatts, Director, Enterprise Security and Architecture, Methodist Health System

SOLUTION OVERVIEW

In order to comply with HIPAA, healthcare organizations and their business partners need to review log data, implement intrusion detection solutions and conduct regular vulnerability scans to help strengthen their security programs and protect PHI. The Alert Logic HIPAA Compliance suite provides broad coverage for HIPAA requirements and keeps health care applications and infrastructure secure. As a managed security and compliance solution based on a SaaS delivery model and a 24 x 7 Security Operations Center, Alert Logic keeps healthcare applications and infrastructure secure without the need for additional resources or lengthy deployment cycles that traditional security solutions require.

THE ALERT LOGIC HIPAA COMPLIANCE SUITE INCLUDES:

ALERT LOGIC® ACTIVEWATCH™

Provides 24x7 security monitoring, expert analysis, and guidance on security events and incidents. This service increases threat detection accuracy, reduces false positives, and allows scarce IT resources to stay focused on business-critical projects. Everything is managed from Alert Logic's state-of-the-art, 24x7 Security Operations Center (SOC), staffed by security professionals with Global Information Assurance Certification (GIAC) from the SANS Institute.

ALERT LOGIC® LOG MANAGER™

Certified security and compliance experts analyze log data to identify potential compliance issues as well as suspicious activity that may indicate a security risk. Organizations can reduce the costs associated with audit preparation, as well as gain deeper visibility into the activity occurring throughout their environments, by using Alert Logic Log Manager to automate the collection, aggregation, and normalization of log data across cloud and on-premises environments.

ALERT LOGIC® THREAT MANAGER™

Detects and prevents network intrusions, identifies vulnerabilities and mis-configurations, and automates security analysis with pre-built alerts and reports for key compliance mandates; backed by security experts who provide detailed remediation guidance as incidents are encountered.

KEY HEALTHCARE INDUSTRY FACTS

- Healthcare data is 50X more valuable on the black market than credit card data.[2]
- The number of HIPAA violation complaints has also geometrically increased since the HITECH act - in the last 3 years; there have been over 70,000 complaints.
- Many of the devices in a healthcare environment are under FDA scrutiny and can't receive Microsoft patches on their needed intervals, nor have their AV signatures updated automatically.

[1] Kaiser Health News, *The Rise Of Medical Identity Theft In Healthcare*, http://bit.ly/1nf7qhe
[2] Government Health IT, *A glimpse inside the $234 billion world of medical fraud*, http://bit.ly/1kZ3KtV | [3] Reuters, *Exclusive: FBI warns healthcare sector vulnerable to cyber attacks*, http://reut.rs/RMogpW

MAPPING TO HIPAA/HITECH REQUIREMENTS:

HIPAA RULE	ALERT LOGIC MAPPING	COVERAGE DETAILS
ADMINISTRATIVE SAFEGUARDS:		
164.308 (A) (1) SECURITY MGMT PROCESS	THREAT MANAGER & ACTIVEWATCH	Risk Analysis (Required) - Integrated Vulnerability Assessment delivers context-aware threat detection and mitigation Risk Management (Required) - Includes the ability to automatically aggregate and correlate anomalous behavior patterns to quickly identify and assess threats and attacks to the network Information system activity review (Required) - Leverages patented expert system, including Threat Scenario Modeling, for more accurate detection
	WEB SECURITY MANAGER & ACTIVEWATCH	Risk Management (Required) - Detect, qualify and assess threats to web applications. Protect business-critical web applications against zero-day exploits and emerging threats and ensures uninterrupted application availability Information system activity review (Required) – Implements policies and procedures to prevent, detect, contain and correct security violations
164.308 (A) (3) WORKFORCE SECURITY	LOG MANAGER & LOGREVIEW	Authorization/supervision (Addressable) - Tracks transitions in availability, and errors, failures and other exceptions in services that archive audit records
164.308 (A) (4) INFORMATION ACCESS MANAGEMENT	LOG MANAGER & LOGREVIEW	Access authorization (Addressable) - Tracks access control changes on users, admin users and groups Access establishment and modification (Addressable) - Shows transition in system availability, shows occurrences of access to audited objects
164.308 (A) (5) SECURITY AWARENESS AND TRAINING	THREAT MANAGER & ACTIVEWATCH	Protection from malicious software (Addressable) - Guards against malicious activity by detecting and preventing network intrusions, identifying vulnerabilities and potential misconfigurations
	WEB SECURITY MANAGER & ACTIVEWATCH	Protection from malicious software (Addressable) - Provides active protection against Web application attacks, including SQL Injection and Cross-Site Scripting attacks
	LOG MANAGER & LOGREVIEW	Protection from malicious activity (Addressable) - Shows occurrences of malware infections, and changes in antivirus availability Log-in monitoring (Addressable) - Shows instances of successful or failed authentication
164.308 (A) (6) SECURITY INCIDENT PROCEDURES	THREAT MANAGER & ACTIVEWATCH	Response & Reporting (Required) - Provides multi-factor, automated real-time detection of threats across environment; Security experts provide detailed remediation guidance on any threat incident identified in the environment
	WEB SECURITY MANAGER & ACTIVEWATCH	Response & Reporting (Required) - Implements policies and procedures to address security incidents; security analysts provide 24x7 monitoring and ongoing tuning, along with escalation for inappropriately blocked requests
164.308 (A) (7) CONTINGENCY PLAN	LOG MANAGER & LOGREVIEW	Data backup plan (Required) - Tracks transitions in database backup service availability, as well as occurrences of database backups
	ACTIVEWATCH FOR THREAT MANAGER, ACTIVEWATCH FOR WEB SECURITY MANAGER	Applications and data criticality analysis (Addressable) - GIAC-certified security experts provide ongoing security tuning in response to changing attacks and customer application changes

HIPAA RULE	ALERT LOGIC MAPPING	COVERAGE DETAILS
PHYSICAL SAFEGUARDS:		
164.310 (A) FACILITY ACCESS CONTROLS	LOG MANAGER & LOGREVIEW	Contingency operations (Addressable) - Logs can be transferred to Alert Logic's secure cloud, thereby preserving them against unauthorized loss, access or modification Access control and validation procedures (Addressable) - Tracks access control changes on users, admin users and groups
164.310 (D) DEVICE AND MEDIA CONTROLS	LOG MANAGER & LOGREVIEW	Data backup and storage (Addressable) - Shows authenticated access by a user to a database, as well as transitions in database backup service availability, and occurrences of database backups
TECHNICAL SAFEGUARDS:		
164.312 (A) (1) ACCESS CONTROL	LOG MANAGER & LOGREVIEW	Unique user identification (Required) - Tracks access control changes on users, admin users and groups Encryption and decryption (Addressable) – Tracks transitions in the availability of, or errors/failures in cryptographic services that provide authentication or privacy
164.312 (B) AUDIT CONTROLS	LOG MANAGER & LOGREVIEW THREAT MANAGER & ACTIVEWATCH	Audit controls - Automates log collection, aggregation and normalization across sources, simplifying log searches and forensic analysis Audit controls - Provides automated security analysis with pre-built alerts and reports for key compliance mandates; visibility into raw events that are directed to or sourced from assets with EPHI data
164.312 (C) INTEGRITY	LOG MANAGER & LOGREVIEW	Mechanism to authenticate electronic PHI (Addressable) - Tracks transitions in the availability of, or errors/failures in services that archive audit records
164.312 (E) TRANSMISSION SECURITY	LOG MANAGER & LOGREVIEW	Encryption (addressable) - Tracks transitions in the availability of, or errors/failures in cryptographic services that provide authentication or privacy
164.310 (A) FACILITY ACCESS CONTROLS	LOG MANAGER & LOGREVIEW	Contingency operations (Addressable) - Logs can be transferred to Alert Logic's secure cloud, thereby preserving them against unauthorized loss, access or modification Access control and validation procedures (Addressable) - Tracks access control changes on users, admin users and groups

THE ALERT LOGIC DIFFERENCE:

DEEP SECURITY INSIGHTS

- BIG DATA ANALYTICS WITH RICH CONTENT
- SECURITY RESEARCH COMBINED WITH EXPERT MONITORING AND SUPPORT
- GLOBAL THREAT VISIBILITY ACROSS THOUSANDS OF CUSTOMERS

CONTINUOUS PROTECTION

- PROTECTION ACROSS ENTIRE APPLICATION STACK, INCLUDING WEB APPLICATIONS
- 24X7 SINGLE-PANE-OF-GLASS VIEW
- CONSISTENT PROTECTION ACROSS CLOUD, HYBRID, AND ON-PREMISES IT

LOWER TOTAL COST

- REDUCED STARTUP COSTS
- NO CAPITAL INVESTMENTS
- OPERATING EXPENSE THAT SCALES WITH THE BUSINESS

ABOUT ALERT LOGIC

Alert Logic, the leader in security and compliance solutions for the cloud, provides Security-as-a-Service for on-premises, cloud, and hybrid infrastructures, delivering deep security insight and continuous protection for customers at a lower cost than traditional security solutions. Fully managed by a team of experts, the Alert Logic Security-as-a-Service solution provides network, system and web application protection immediately, wherever your IT infrastructure resides. Alert Logic partners with the leading cloud platforms and hosting providers to protect over 3,300 organizations worldwide. Built for cloud scale, our patented platform stores petabytes of data, analyses over 400 million events and identifies over 50,000 security incidents each month, which are managed by our 24x7 Security Operations Center. Alert Logic, founded in 2002, is headquartered in Houston, Texas, with offices in Seattle, Dallas, Cardiff, Belfast and London. For more information, please visit www.alertlogic.com.

ALERT LOGIC®