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 24/7 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:

## 24/7 SECURITY MONITORING

Provides 24/7 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, 24/7 Security Operations Center (SOC), staffed by security professionals with Global Information Assurance Certification (GIAC) from the SANS Institute.

## MANAGED WEB APPLICATION SECURITY

Proactive defense against web application attacks, providing immediate protection against zero-day attacks that signatures cannot detect and is backed by the 24/7 Security Operations Center that monitors all activity and ongoing WAF tuning to optimize protection, removing the biggest challenge of WAF utilization.

## LOG MANAGEMENT

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

## 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.

## THREAT DETECTION

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

[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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 |
| | ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Protection from malicious software (Addressable) - Guards against malicious activity by detecting and preventing network intrusions, identifying vulnerabilities and potential misconfigurations |
| | ALERT LOGIC ENTERPRISE | Protection from malicious software (Addressable) - Provides active protection against Web application attacks, including SQL Injection and Cross-Site Scripting attacks |
| | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 |
| | ALERT LOGIC ENTERPRISE | Response & Reporting (Required) - Implements policies and procedures to address security incidents; security analysts provide 24/7 monitoring and ongoing tuning, along with escalation for inappropriately blocked requests |
| 164.308 (A) (7) CONTINGENCY PLAN | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Data backup plan (Required) - Tracks transitions in database backup service availability, as well as occurrences of database backups |
| | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Applications and data criticality analysis (Addressable) - GIAC-certified security experts provide ongoing security tuning in response to changing attacks and customer application changes |

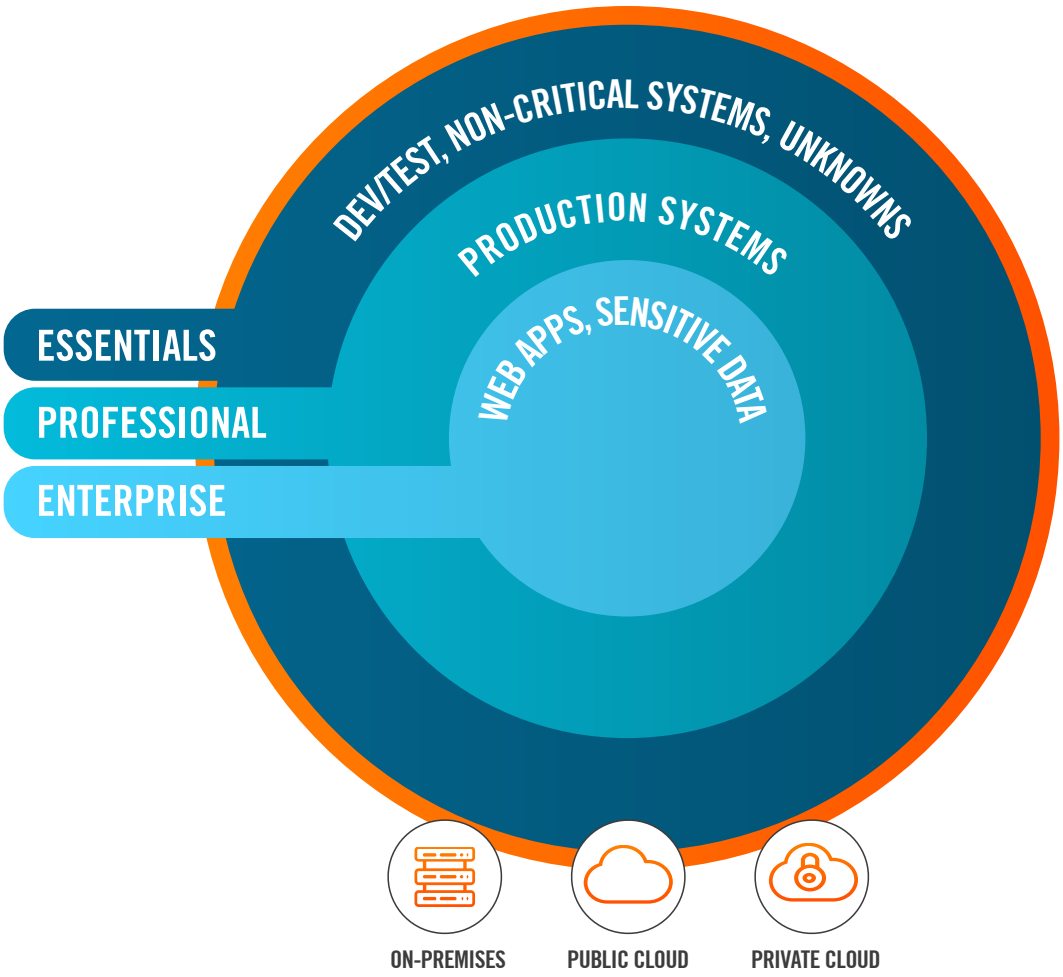
| HIPAA RULE | ALERT LOGIC MAPPING | COVERAGE DETAILS |
|---|---|---|
| PHYSICAL SAFEGUARDS: | | |
| 164.310 (A) FACILITY ACCESS CONTROLS | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Contingency operations (Addressable) - Logs can be transferred to Alert Logic's secure cloud, thereby preserving them against unauthorized loss, access or modification<br><br>Access control and validation procedures (Addressable) - Tracks access control changes on users, admin users and groups |
| 164.310 (D) DEVICE AND MEDIA CONTROLS | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Unique user identification (Required) - Tracks access control changes on users, admin users and groups<br><br>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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Audit controls - Automates log collection, aggregation and normalization across sources, simplifying log searches and forensic analysis |
| | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | 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 | ALERT LOGIC PROFESSIONAL, ALERT LOGIC ENTERPRISE | Contingency operations (Addressable) - Logs can be transferred to Alert Logic's secure cloud, thereby preserving them against unauthorized loss, access or modification<br><br>Access control and validation procedures (Addressable) - Tracks access control changes on users, admin users and groups |

ALERT LOGIC®

## *SIEM*LESS THREAT MANAGEMENT

PLATFORM | INTELLIGENCE | EXPERTS

The Right Coverage for the Right Resources




SIEMless by Design | Any Environment | Lower Total Cost | Always Advancing



ALERT LOGIC®