ALERT LOGIC™

SOLUTION BRIEF

Alert Logic Security Compliance

Compliance is a challenge for many organizations as stretched security and IT staff struggle to keep up with requirements that seem to constantly evolve. Regulators continue to impose compliance rules to protect organizations, individuals and industry groups from data breaches and data loss. One result of this is that companies are allocating 14.3% on average of their IT budget to compliance spending. And, the cost of non-compliance can be 2.7 times higher than the cost of compliance due to business disruption, revenue losses, fines, and settlement costs.1

THE COST BURDEN IS INCREASED WITH THE NEED TO FIND AND RETAIN DEDICATED PROFESSIONAL STAFF, AND TO IMPLEMENT TECHNOLOGIES TO CURTAIL RISK.

It's time think differently. The traditional way has organizations increasing their security spend each year yet they are not getting closer to achieving the compliance outcomes. Traditional security tools and point products continue generate a myriad of alerts which require highly skilled expertise which is in short supply in order to get value. Organizations want a simpler way meet compliance across multiple regulations without having to hire and train additional staff.

2.7x

higher cost for non-compliance than the cost of compliance

14%

average of a companies IT budget allocated to compliance

Why Alert Logic for Compliance?

- We help organizations achieve compliance with minimal disruption with a security and threat management platform and expert staff support for any environment
- Our experts will filter out the noise and investigate and respond to incidents that could lead to a business being out of compliance
- We provide services 24 hours a day, every day of the year—offloading the high costs of in-house security staff
- Our SOC provides security experts who will review incidents and provide additional context and remediation actions based on knowledge gathered from thousands of incidents
- We work personally with each customer to provide personal notifications. Our analysts call, text or email you within 15 minutes of high- and critical-priority attacks

Alert Logic Security Compliance Benefits

- Quickly understand state of compliance without hiring new staff
- Audit-ready reporting that helps IT staff stay one step ahead of requirements, mandates and auditors
- Improved security posture, reduced attack surface and risk of data breach
- Get informed advice and remediation steps from our security experts
- Streamlined governance processes, and build compliance controls directly into IT processes
- Build trust with your stakeholders, customers and prospects by providing proof to stakeholders who require it
- Take the lead over competitors by offering proof of compliance where your prospects are likely to appreciate your above-and-beyond approach to business precautions

"Using Alert Logic's managed threat defense solution in conjunction with our other security measures, helped us to demonstrate compliance with the PCI Data Security Standard and pass the audit"

Wyman Lewis, Director of Information Security, GSI Commerce

gsi commerce®

"It made it very easy for us to check the boxes and make sure we are covered without having to invest a whole lot in new personnel"

Bill Thornton, Vice President, Tango

TANGO

Alert Logic Solutions Compliance Mapping

OFFERINGS	PCI DSS 3.2	HIPAA & HITECH	SOC 2 (TSP 100)
Alert Logic Professional Includes Essentials 24/7 Managed Threat Detection and Incident Management - 24/7 Incident Monitoring & Management - Security Analytics & Threat Intelligence - Log Collection and Monitoring - Intrusion Detection - Security Event Insights and Analysis - Office 365 Log Collection & Search - Cloud Vendor Security Integrations - AWS User Behavior Anomaly Detection - Anti-Virus Integration	10.1 - Implement audit trails 10.2 - Automated audit trails 10.3 - Capture audit trails 10.5 - Secure logs 10.5.5 - Change detection to ensure integrity for log files 10.6 - Review logs 10.7 - Maintain logs online 10.7 - Retain audit trail 10.8.1 - Respond to failures of critical security controls 11.4 - Use intrusion-detection and/or intrusion-prevention techniques 11.5 - Change detection to ensure integrity for critical system files, configuration files, or content files 12.10.1 - Implement an incident response plan	164.308 (a)(1)(ii)(B) - Risk Management 164.308 (a)(1)(ii)(D) - Information System Activity 164.308 (a)(4)(i) - Information Access Management 164.308 (a)(5)(ii)(B) - Protection from Malicious Software 164.308 (a)(5)(ii)(C) - Login Monitoring 164.308 (a)(6)(ii) - Response & Reporting 164.312 (a) - Access Control 164.312 (b) - Audit Controls 164.312 (c)(1)(2) - Protect from improper alteration or destruction and confirm integrity	CC 6.2 - User Registration CC 6.3 - Access Modification CC 7.2 - Security Event and Anomaly Detection CC 7.3 - Incident Detection and Response
Alert Logic Essentials Vulnerability & Asset Visibility - Asset Discovery - Vulnerability Scanning - Cloud Configuration Checks - Endpoint Detection - Threat Risk Index - Compliance Scanning and Reporting	6.1 - Identify vulnerabilities 11.2 - Perform network vulnerability scans by an ASV (Includes 11.2.1, 11.2.2 and 11.2.3)	164.308 (a)(1) - Security Management Process 164.308 (a)(1)(i)(A) - Risk Analysis	CC 3.2 - Risk Identification CC 6.6 - External Threats CC 6.8 - Unauthorized and Malicious Code Protection CC 7.1 - Vulnerability Management
Alert Logic Enterprise Includes Professional Designated Security Expert - Continuous Threat Hunting - Pro-Active Tuning and Sensor Optimization - Weekly Security Review			

Alert Logic Solutions Compliance Mapping (CONT.)

	GDPR	SOX 404
Alert Logic Professional **Includes Essentials** 24/7 Managed Threat Detection and Incident Management - 24/7 Incident Monitoring & Management - Security Analytics & Threat Intelligence - Log Collection and Monitoring - Intrusion Detection - Security Event Insights and Analysis - Office 365 Log Collection & Search - Cloud Vendor Security Integrations - AWS User Behavior Anomaly Detection - Anti-Virus Integration	Article 34 - Communication of a personal data breach	DS 5.5 - Security Testing, Surveillance and Monitoring DS 5.6 - Security Incident Definition DS 13.3 - IT Infrastructure Monitoring
Alert Logic Essentials Vulnerability & Asset Visibility - Asset Discovery - Vulnerability Scanning - Cloud Configuration Checks - Endpoint Detection - Threat Risk Index - Compliance Scanning and Reporting	Article 24 - Responsibility of the controller Article 25 - Data protection by design and by default Article 32 - Security of processing Article 35 - Data protection impact assessment	DS 5.9 - Malicious Software Prevention, Detection and Correction
Alert Logic Enterprise **Includes Professional** Designated Security Expert - Continuous Threat Hunting - Pro-Active Tuning and Sensor Optimization - Weekly Security Review		

Alert Logic Solutions Compliance Mapping (CONT.)

OFFERINGS	ISO 27001/27002	NIST 800-171	NIST 800-53
Alert Logic Professional Includes Essentials 24/7 Managed Threat Detection and Incident Management - 24/7 Incident Monitoring & Management - Security Analytics & Threat Intelligence - Log Collection and Monitoring - Intrusion Detection - Security Event Insights and Analysis - Office 365 Log Collection & Search - Cloud Vendor Security Integrations - AWS User Behavior Anomaly Detection - Anti-Virus Integration	12.2 - Protection from malware. 12.4 - Logging and monitoring. 16.1 - Management of information security incidents and improvements	3.5 - Identification and Authentication 3.6 - Incident Response	CA-2 Security Assessments CA-3 Information System Connections CA-7 Continuous Monitoring IR-5 Incident Monitoring IR-6 Incident Reporting IR-7 Incident Response Assistance SC-7 Boundary Protection SI-3 Intrusion Detection Tools and Techniques SI-4 The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system SI-5 Security Alerts And Advisories SI-7 Software And Information Integrity
Alert Logic Essentials Vulnerability & Asset Visibility - Asset Discovery - Vulnerability Scanning - Cloud Configuration Checks - Endpoint Detection - Threat Risk Index - Compliance Scanning and Reporting	8.1 - Responsibility for assets 12.6 - Technical vulnerability management	3.1 - Access Control 3.3 - Audit and Accountability 3.4 - Configuration Management 3.11 - Risk Assessment 3.12 - Security Assessment 3.13 - System and Communications Protection 3.14 - System and Information Integrity	RA-3 Risk Assessment RA-5 Vulnerability Scanning
Alert Logic Enterprise Includes Professional Designated Security Expert - Continuous Threat Hunting - Pro-Active Tuning and Sensor Optimization - Weekly Security Review			