ALERT LOGIC®

CHEAT SHEET:

PCI DSS 3.1 COMPLIANCE

WHAT IS PCI DSS?

- Payment Card Industry Data Security Standard
- Information security standard for organizations that handle data for debit, credit, prepaid, e-purse, ATM, and POS card brands
- Standard to increase controls around cardholder data protection and reduce credit card fraud

12 REQUIREMENTS:

CONTROL OBJECTIVES	PCI DSS REQUIREMENTS
BUILD AND MAINTAIN A SECURE NETWORK	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
PROTECT CARDHOLDER DATA	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	5. Use and regularly update antivirus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
IMPLEMENT STRONG ACCESS CONTROL MEASURES	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
REGULARLY MONITOR AND TEST NETWORKS	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
MAINTAIN AN INFORMATION SECURITY POLICY	12. Maintain a policy that addresses information security

WHO NEEDS TO BE PCI DSS COMPLIANT?

- All entities involved in payment card processing
- There are four compliance levels, based on the number of transactions a merchant processes each year:
  - Separate levels for Visa®, MasterCard® and service providers
  - PCI training and reporting requirements for merchants depends on compliance level
  - Annual compliance validation, either through a Self-Assessment Questionnaire (SAQ) or a Qualified Security Assessor (QSA), depending on compliance level

WHAT HAPPENS IF AN ORGANIZATION DOESN'T COMPLY?

- Increased risk of payment card data compromise
- Subject to fines
- Loss of credit card acceptance privileges

HOW DO ALERT LOGIC SOLUTIONS ADDRESS PCI DSS?

Alert Logic addresses an important subset of the PCI DSS requirements:

THREAT MANAGER™ WITH ACTIVEWATCH provides IDS and vulnerability scanning for specific compliance requirements, and reporting for customer compliance. ActiveWatch for Threat Manager adds 24×7 monitoring of network traffic by security analysts for rapid detection and response.

LOG MANAGER™ WITH ACTIVEWATCH collects and normalizes log data from the entire IT infrastructure and presents it in a single view, through a web interface that includes 100+ pre-built reports and powerful analytical tools. LogReview service adds daily reporting by expert security analysts extract meaning from vast amounts of log data. ActiveWatch service provides 24x7 monitoring to prevent future breaches through automated post compromise detection.

CHANGES IN PCI DSS: 3.1 UPDATE – APRIL 2015

- The primary change for 3.1 was to specify that older versions of SSL and TLS are not secure. Alert Logic identifies the older protocols as vulnerabilities, and our appliances can only communicate with our backend environment that uses TLS 1.2, a secure version.

MORE SPECIFIC CHANGES INCLUDE:

- 6.6 – Added clarification to response time on automated solutions for web-based attacks
- 10.6 – Redundant language removed for added clarification
- 11.2 – Vulnerability scan can be a combination of automated and manual tools, techniques, or other methods

WHAT WERE THE SIGNIFICANT CHANGES IN PCI DSS 3.0?

- The theme of 3.0 was the evolution of security compliance from a once-a-year event to a day-to-day practice. While this has been the case for some time, the new standard made it more explicit.

NEW REQUIREMENTS INCLUDE:

- 2.4 – Maintain inventory of system components in scope for PCI DSS
- 5.1.2 – For systems not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats
- 9.9 – Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution
- 11.3 – Implement an industry-accepted methodology for penetration testing
- 12.8.5 – Maintain information about which PCI DSS requirements are met by each service provider, and which are managed by the entity

PCI DSS FREQUENTLY ASKED QUESTIONS

QUESTION	ANSWER
Is Alert Logic a PCI DSS Approved Scanning Vendor (ASV)?	Yes. Alert Logic maintains ASV status.
With which requirements can Alert Logic help me?	Threat Manager and the associated ActiveWatch service: 6.1, 11.2 (including 11.2.1, 11.2.2, and 11.2.3), and 11.4 Log Manager, LogReview, and the associated ActiveWatch service: 10.2, 10.3, 10.5, 10.6, and 10.7 Web Security Manager and the associated ActiveWatch service: 6.5, 6.6
What kind of responsibilities do customers have to make Alert Logic products and services address PCI DSS requirements?	Alert Logic customers must ensure that the products are monitoring the correct sources, and when Alert Logic notifies customers of issues in their environment, the customer must address the issues quickly. Also, customers are responsible for ensuring that the logs and other information sent to Alert Logic does not contain credit card data or any associated personal information. Details of these requirements are communicated in the contracts and during the Alert Logic onboarding and provisioning processes.
Does Alert Logic store logs long enough for PCI DSS requirements?	Yes. Alert Logic stores logs for a minimum of one year. Customers have the options of extended that time period, but only by contract, not by settings in the user interface.
I've seen several documents referring to Alert Logic as a PCI DSS Service Provider. What does that term mean?	The PCI Security Standards official glossary defines "Service Provider" as: "Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although it may be considered a service provider for other services)."
If I'm being audited, how can Alert Logic make the process easier?	Alert Logic provides reports that customers can give to their QSA. We can also answer questions about our services and appliances.

HELPFUL LINKS

ALERT LOGIC INFORMATION: http://www.alertlogic.com/pci-dss

PCI SECURITY STANDARDS COUNCIL: https://www.pcisecuritystandards.org/

VISA CARDHOLDER INFORMATION SECURITY PROGRAM: http://usa.visa.com/merchants/risk_management/cisp_overview.html

MASTERCARD SITE DATA PROTECTION PROGRAM: http://www.mastercard.com/us/company/en/whatwedo/site_data_protection.html

AMERICAN EXPRESS DATA SECURITY STANDARD:

https://www.americanexpress.com/in/content/merchant/support/data-security/merchant-information.html

DISCOVER INFORMATION SECURITY AND COMPLIANCE: http://www.discovernetwork.com/merchants/data-security/disc.html

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®

0915US