SageNet
CONNECT | MANAGE | PROTECT

PCI SOLUTIONS

Compliance and Beyond

Mandated by card issuers, PCI DSS requires all merchants with internal systems that store, process or transmit cardholder data to comply with key data protection measures and submit to annual security audits. SageNet offers a variety of cybersecurity and compliance services that help merchants achieve compliance with PCI mandates. What's more, SageNet cybersecurity services can help your organization go beyond compliance to achieve a true enterprise-wide culture of information security.

CYBERSECURITY SERVICES

Managed Authentication

PCI Requirements 7 & 8

SageNet offers a Software Defined Perimeter managed service that enables secure authentication to enforce "zero trust" network and application level access controls.

SIEMaaS

PCI Requirement 10

SageNet's SIEM as a Service incorporates a SIEM deployment, configuration and maintenance to deliver data log aggregation, security event correlation and SageNet's security content suite.

SOCaaS

PCI Requirement 10.6

US-based 24x7x365 Security Operations Centers continuously monitor, investigate and escalate security events. Includes the SIEM, log collection, custom security content and monitoring service.

Penetration Tests

PCI Requirement 11.2

Identify vulnerabilities to harden defenses. Testing capabilities include internal, external, web application, mobile, physical and social engineering.

ASV Scanning

PCI Requirement 11.2.2

Approved Scanning Vendor (ASV) services to externally scan customer environments with the purpose of identifying vulnerabilities for remediation.

Security Assessments

PCI Requirement 12.2

Security program assessment services based on standard security frameworks of ISO 27001/27002, NIST 800-53 and PCI DSS compliance.

sageSECURE.™

PCI Compliance Integrated within SageNet's CompleteConnect™

Firewall Configuration, Design, Review and Management

PCI Requirement 1.1.7

- SageNet's Managed Network Service is rooted in the design, configuration, and management of Unified Threat Management (UTM) appliances and firewalls to build and operate a secure managed network 24x7x365.

Security VPN Transport Encryption

PCI Requirement 4

- SageNet's CompleteConnect™ services encrypt data in transport for more secure and PCI compliant data communication.

Data Center Security – Physical and Logical

PCI Requirement 9

- SageNet data centers across the US utilize stringent physical security controls that restrict access at multiple levels and allow for physical monitoring of the environment.

PCI Compliant Network Management

PCI Requirement 10.8

- SageNet undergoes an annual PCI audit to validate the controls and processes that are in place to remain a PCI compliant service provider.

Continuous SIEM Monitoring of SageNet Internal Hosts

PCI Requirement 10.6 and 12.11

- SageNet's internal security program utilizes a SIEM for internal security event data monitoring.

Annual Assessment

Annual Assessment: Attestation of Compliance (AOC)

- Each year, SageNet undergoes a rigorous audit to ensure that all security controls and process are adhering to the latest PCI DSS compliance standards.

SageNet
CONNECT | MANAGE | PROTECT

To learn more about SageNet's PCI Compliance Solutions, visit www.sagenet.com or call 1-866-480-2263.