PCI-DSS Compliance Reports

Simplify PCI Compliance with the AWN CyberSOC™ Service

AWN CyberSOC™ Service

- Superior managed threat detection and response
- Dedicated security expertise for your IT team
- 24/7 monitoring with unlimited log sources

Benefits

- Simplifies PCI-DSS 3.2 compliance with customized reporting
- Monitors access to cardholder data on-premises and in the cloud
- Provides real-time alerts based on business risks posed by payment card data

With the widespread use of payment cards for online shopping, banking, and other business transactions, credit card data exposure and fraud is on the rise. To combat this growing menace, the Payment Card Industry Data Security Standard (PCI-DSS) was developed in 2006 by leading credit card institutions like Visa and MasterCard. PCI-DSS mandates all organizations that accept, transmit, process and store cardholder data must continuously monitor and safeguard all sensitive customer information. These regulations apply to organizations of all sizes, including small and medium-sized banks, credit unions, medical clinics, law offices and other merchants that handle payment card transactions.

Arctic Wolf's security operations center (SOC)-as-a-service enables companies to meet certain PCI-DSS compliance requirements using the industry-leading, cloud-based AWN CyberSOC. Arctic Wolf simplifies compliance reporting, customizing reports to meet your business needs with the help of our dedicated Concierge Security™ team assigned to your account.

PCI-DSS Compliance Requirements

Cardholder information may be stored in a variety of repositories, such as file servers, databases, access logs, and other types of unstructured and structured data repositories. Safeguarding cardholder data in these repositories in a manner compliant with PCI DSS requires diligent administration and close cooperation between IT teams and the many business units that need access to the data.

Finding the right balance between the tasks that can be supported by your IT organization and the checks that can be automated through Arctic Wolf's SOC-as-a-service enables you to streamline PCI-DSS compliance and reduce overall cost.

The Primary Requirements of PCI DSS Are:

Objective:	Requirement:
Build and maintain a secure network	Monitor changes to firewall configurations and use of default passwords
Protect cardholder data	Monitor cardholder data, at rest and in motion, to ensure it doesn't go to malicious IP addresses/locations
Maintain a vulnerability management program	Regularly run vulnerability scans on Internet-facing systems that process cardholder data
Implement strong access control measures	Monitor all login activity with integration to Active Directory services and monitor anomalous user behavior
Regularly monitor and test networks	Continuously monitor network traffic 24/7, and regularly assess network for vulnerabilities
Maintain an information security policy	Focus on incident detection and response and monitor incident response workflow to closure

Arctic Wolf Compliance Solution for PCI-DSS

Arctic Wolf's AWN CyberSOC™ service monitors all activity in on-premises IT infrastructure and cloud applications using physical/virtual AWN sensors. AWN CyberSOC continuously monitors network flows and ingests log records from an unlimited number of log sources. It uses human-augmented machine learning to accurately detect and respond to advanced attacks.

The Arctic Wolf Concierge Security™ team (CST) dedicated to each customer account augments your IT staff's security expertise, hunts down advanced zero-day attacks, identifies PCI violations, and provides customized compliance reports to meet your PCI-DSS requirements. The table below shows how AWN CyberSOC enables you to address each section of the 12 PCI-DSS requirements.

	Requirement	Arctic Wolf Solution
PCI-DSS 1: Install and maintain firewall configuration to protect data	Collect logs from firewall devices to ensure and validate compliance	Arctic Wolf monitors all used services, protocols, and ports, validates inbound and outbound traffic, and captures event alerts related to network and firewall activity
PCI-DSS 2: Do not use vendor-supplied defaults for system passwords and security parameters	Monitor network for anomalous behavior and signs of insufficient configuration	Arctic Wolf provides a record of all network services used and alerts on use of unauthorized services and insecure protocols
PCI-DSS 3: Protect stored cardholder data	Monitor changes in cardholder environment and alert on changes to critical services	Arctic Wolf monitors activity on all systems that handle cardholder data, and alerts on anomalous network connections to malicious IPs or geo-locations
PCI-DSS 4: Encrypt transmission of cardholder data across open, public networks	Monitor network usage to ensure proper network protocols are used in cardholder environments	Arctic Wolf monitors and alerts when unauthorized or unencrypted services are used; it can detect unauthorized wireless access points

› Arctic Wolf Compliance Solution for PCI-DSS (Continued)

	Requirement	Arctic Wolf Solution
PCI-DSS 5: Protect all systems against malware and regularly update AV software	Alert on vulnerabilities and advanced malware from log data collected from endpoint protection solutions	Arctic Wolf scans endpoints for unpatched vulnerabilities, and collects logs from endpoint security solutions when advanced malware is detected
PCI-DSS 6: Develop and maintain secure systems and applications	Monitor for vulnerabilities and software update activity to help organizations develop and maintain secure systems	Arctic Wolf regularly scans systems for unpatched vulnerabilities and provides a status report for the security posture of all applications, systems and security devices
PCI-DSS 7: Restrict access to cardholder data by business need-to-know	Monitor access privilege assignments and suspicious data access	Arctic Wolf collects relevant data from access control systems and the Active Directory, monitoring and validating access to cardholder data and system components through account creation, object access, privilege assignment and revocation
PCI-DSS 8: Identify and authenticate access to system components	Identify shared account usage in the network, especially privileged accounts with more than one user	Arctic Wolf monitors Active Directory logs, and reports on all user account activity from account creation to account removal; AWN also alerts on shared account usage
PCI-DSS 9: Restrict physical access to cardholder data	Monitor physical access control devices for access attempts to areas hosting cardholder data	Arctic Wolf alerts on physical access failures and details on other physical access activities, by integrating logs generated by those devices
PCI-DSS 10: Track and monitor all access to network resources and cardholder data	Automate collection, centralization and monitoring of logs from servers, applications, security and other devices	Arctic Wolf collects and aggregates access-related logs from multiples devices/systems and network flow data on sensors; these logs are sent securely to the cloud-based AWN CyberSOC which analyzes and detects advanced threats to systems that handle cardholder data
PCI-DSS 11: Regularly test security systems and processes	Collect logs from IDS/IPS systems to ensure and validate compliance	Arctic Wolf sensors deployed on customer premises include IDS/IPS functionality to generate real-time alerts on intrusion-related activity
PCI-DSS 12: Maintain a policy that addresses information security	Provide centralized visibility and control to support organizational security policies, including incident handling and response	Arctic Wolf CyberSOC has centralized security policies that can be customized by the AWN Concierge Security™ team to meet the compliance reporting needs of the customer

AUTHORIZED PARTNER
THE INFORMATION STRATEGISTS

The Information Strategists, LLC
info@informationstrategists.com
https://theinformationstrategists.com