Kiteworks

COMPLIANCE BRIEF

Kiteworks Boasts a PCI DSS Compliant Platform

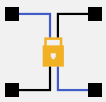
Robust Security Features for Protecting Cardholder Data

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It applies to any organization, regardless of size or number of transactions, that handles cardholder data, including industries such as retail, banking, finance, insurance, and any business processing payments. Noncompliance can result in hefty fines, increased transaction fees, damage to reputation, and even the loss of the ability to process credit card payments. The 12 key requirements of PCI DSS cover areas such as installing and maintaining network security controls, applying secure configurations to system components, protecting stored account data and cardholder data during transmission, protecting systems from malicious software, developing secure systems and software, restricting access, identifying users, authenticating access, logging and monitoring, testing security, and supporting information security with organizational policies and programs. Kiteworks is a PCI DSS compliant platform and supports compliance. Here's how:

Strong Security Foundation With a Hardened Virtual Appliance

Secure network and systems requirements collectively help establish a robust security foundation by installing and maintaining firewalls, avoiding default passwords, protecting against malware, and developing secure systems and applications. The Kiteworks platform meets PCI DSS requirements for secure network and systems by leveraging AWS and utilizing single-tenant private clouds to protect cardholder data. The platform operates on a least-privilege default, ensuring that only necessary traffic is permitted. Kiteworks is a pre-hardened appliance where all connectivity to the system is through secure channels utilizing encryption. Finally, antivirus and vulnerability mitigation is deployed to all servers and changes to the production environment follow a documented change management process, requiring management review and approval. These features collectively create a strong security foundation for the Kiteworks platform.

Solution Highlights

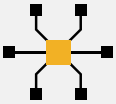


Robust access controls

Single-tenant private cloud

Double encryption

Customer-owned keys



SIEM integration

Robust Access Control and Encryption Secure Data

Requirements surrounding data protection and access control ensure sensitive data remains secure and accessible only to authorized personnel by protecting stored data, encrypting transmitted data, restricting access based on need-to-know, assigning unique IDs, and restricting physical access. Kiteworks protects stored cardholder data by encrypting data at rest with AES-256, data in transit is encrypted with TLS 1.3, and with customers responsible for managing their own encryption keys. Access to sensitive data is controlled by customers with built-in authentication and integration with existing identity providers as well as granular access controls. Each user account is assigned a unique ID, and the customer configures password security requirements. This ensures sensitive data remains secure and accessible only to authorized personnel.

Monitor and Identify Potential Gaps in Real Time

Final requirements involve monitoring, testing, and policy to help organizations stay vigilant, identify potential security gaps, and foster a culture of security awareness and responsibility by tracking and monitoring access, regularly testing security systems and processes, and maintaining an information security policy for all personnel. The platform provides SIEM integration and log forwarding, and audit logs capture all user access, changes to accounts, and authentication settings in real time with log files made immutable by design. Kiteworks also manages vulnerability scans, bounty programs, and third-party penetration tests, which are conducted regularly. These features help organizations stay vigilant, identify potential security gaps, and foster a culture of security awareness and responsibility among employees.

Kiteworks is a PCI DSS compliant platform that offers a comprehensive set of security features to protect cardholder data. The platform leverages a hardened virtual appliance, secure data encryption, and robust access controls to ensure that sensitive information remains secure and accessible only to authorized personnel. Kiteworks also provides real-time monitoring and log forwarding to help organizations stay vigilant and identify potential security gaps. With regular vulnerability scans, bounty programs, and third-party penetration tests, Kiteworks ensures that its platform remains secure and compliant with the latest PCI DSS requirements. By utilizing Kiteworks, organizations can maintain a secure environment for processing credit card transactions while reducing the risk of data breaches and noncompliance penalties.