Kiteworks

COMPLIANCE BRIEF

Empower PCI Compliance and Secure Data Management With Kiteworks

Harness Robust Features and Advanced Security Measures to Safeguard Cardholder Data and Ensure PCI DSS Compliance

PCI (Payment Card Industry) refers to the standards and regulations set forth by major credit card companies to ensure the secure handling of cardholder data during payment transactions. The PCI standards, specifically the Payment Card Industry Data Security Standard (PCI DSS), provide a comprehensive framework for organizations to protect sensitive credit card information. Compliance with PCI DSS is essential for businesses that process, store, or transmit credit card data. It encompasses requirements such as maintaining a secure network, protecting cardholder data, implementing access controls, regularly monitoring and testing systems, and maintaining information security policies. By adhering to PCI standards, organizations can mitigate the risk of data breaches, fraud, and financial penalties while safeguarding the trust and confidence of customers. Kiteworks can help organizations maintain compliance with the PCI DSS by providing a secure platform for managing, sharing, and storing sensitive data, including cardholder information. Kiteworks provides secure content communication and data management capabilities that support organizations in meeting some of the PCI DSS requirements. Here are some ways Kiteworks can contribute to PCI DSS compliance:

Embedded Firewall Configuration Protects Cardholder Data

Kiteworks brings significant value to organizations striving for PCI compliance through its embedded network firewall and web application firewall (WAF). With an embedded WAF and network firewall actively defending against web-based attacks on every Kiteworks web node, enhanced security is ensured. The hardened virtual appliance ensures enhanced security by opening only necessary ports in the embedded network firewall and employing least-privilege access controls to protect content within internal tiers of services. Furthermore, Kiteworks actively monitors and blocks malicious connections through its embedded intrusion prevention system (IPS) and malicious web requests via its embedded WAF. This robust combination of network firewall, access controls, IPS, and WAF provides organizations with a powerful defense against cyber threats, helping them meet PCI requirements and safeguard sensitive data.

Solution Highlights

- Embedded firewall configuration
- System password security and authentication integration
- Encryption of stored and transmitted data
- Secure systems development
- Comprehensive access tracking and monitoring
- Compliance risk management

System Password Security Enforced With Policies and Storage

Kiteworks integrates with customers' standard identity management systems and authentication systems such as LDAP, Microsoft AD and Azure AD, RADIUS multi-factor authentication, OAuth, SAML 2.0, etc. It also provides native password management for users not in corporate identity management systems, such as third-party users. Administrators have full control over the password policy, including length, character requirements, expiration, and history. By default, Kiteworks ensures secure authentication by storing username and password credentials in a secure database. To further enhance security, Kiteworks employs salting and hashing algorithms for password storage. Administrators can enforce policies to strengthen password security, such as minimum length and character combinations, password expiration, disallowing password reuse, and disabling autofill. These robust features enable organizations to meet PCI compliance requirements while bolstering overall security.

Encrypt Stored Cardholder Data

The platform prioritizes the security of sensitive content by implementing encryption both in transit and at rest. This ensures that files being transferred between users or stored on the platform are encrypted, providing robust protection against unauthorized access. Moreover, Kiteworks grants organizations ownership of their encryption keys, empowering them with control over key management for enhanced security. With these encryption features in place, Kiteworks ensures the privacy and integrity of data shared and stored within its platform, enabling organizations to meet PCI encryption compliance while safeguarding their sensitive information.

Encrypt Transmissions of Cardholder Data

The platform utilizes encrypted HTTPS/TLS connections to establish secure communication between the client and the Kiteworks server. TLS (Transport Layer Security) is a widely adopted cryptographic protocol known for providing robust security during network communication. By implementing TLS, which is an enhanced and more secure iteration of SSL (Secure Sockets Layer), Kiteworks ensures that data transmitted between users and the platform remains confidential and shielded from unauthorized access or tampering. This encryption measure ensures the protection and integrity of cardholder data within the Kiteworks environment, helping organizations meet the stringent encryption standards mandated by PCI.

Deploy and Maintain Antivirus Software

The platform offers a built-in F-Secure® antivirus (AV) service option, which conducts comprehensive malware scans on files during both download and upload processes. This crucial feature serves as a protective measure, ensuring the security of shared content within the Kiteworks environment. Files of any size, including those passing through Enterprise Connect sources or the Email Protection Gateway (EPG), can be scanned for malware. Kiteworks allows administrators to configure settings, enabling them to quarantine infected files or log and alert accordingly. Moreover, Kiteworks stays up to date by incorporating the latest version of WithSecure Atlant antivirus software, providing enhanced protection against malware and viruses. Kiteworks servers regularly connect to WithSecure servers to automatically download the latest antivirus updates to ensure you always have up-to-date protection. This robust antivirus functionality helps organizations meet PCI requirements and fortify their defenses against potential threats.

Develop and Maintain Secure Systems

Flexible deployment options, including on-premises, private cloud hosted, FedRAMP, and IRAP, help customers meet their security policies. With Kiteworks, organizations minimize their entire attack surface because it encloses all system components in a hardened virtual appliance.

Security is bolstered by Kiteworks' secure development life cycle, including secure coding practices, secure software supply chain practices, regular penetration testing, and a worldwide bounty program that eliminates bugs before they become vulnerabilities. Finally, one push of a button updates all the system components so organizations never miss a patch. By following these practices, Kiteworks develops and maintains secure systems and appliances for PCI compliance, enabling organizations to securely share and collaborate on content.

Provide Access Privileges

The platform utilizes a granular, least-privilege permission system, allowing administrators to control user access to shared resources. Content access privileges are assigned based on roles for each set of information on a need-to-know basis, such as Folder Owner, Manager, Collaborator, Downloader, Uploader, or Viewer, and expiration is automatically enforced. User roles also define access to functionality such as content storage and data transfer, clients such as mobile devices, domains and IP ranges for data transfers, and many other factors. This ensures that sensitive information is accessible only to authorized users, fostering a secure environment for collaboration, while maximizing protection. Kiteworks also provides governance controls, unified security, and a comprehensive audit log to aid in compliance and risk management. With its strong access privilege management, Kiteworks empowers organizations to meet PCI requirements, protect sensitive data, and maintain control over content collaboration.

Protect Cardholder Data With Unique User IDs to Authenticate Individuals

Each user is assigned a unique user ID, ensuring accountability and traceability for all system actions. Kiteworks offers multiple authentication options, including password-based authentication where users sign in with their unique user ID and a strong password. Certificate-based authentication is also supported, allowing users to sign in using trusted certificates installed in their browsers. Additionally, Kiteworks supports two-factor authentication (2FA) or multi-factor authentication (MFA), including RADIUS 2FA/MFA, native OTP-based 2FA, and OAuth. By implementing unique user IDs and diverse authentication methods, Kiteworks ensures that only authorized users can access the platform, providing a secure environment for sharing and collaborating on sensitive cardholder data.

Restrict Physical Access to Cardholder Data

Systems hosted by Kiteworks provide physical access restrictions inherited from the Amazon AWS or Microsoft Azure environments where Kiteworks hosts its virtual appliances. These restrictions include physical access to employees and contractors based on approved business justifications. They are granted least-privilege, time-bound access to specific layers of the data center, enforced by the use of badges and authorized AWS or Azure staff. Third parties who are granted access must be escorted by authorized staff. Amazon further restricts physical access to data centers in AWS GovCloud (U.S.), which Kiteworks uses to host its FedRAMP offering, to employees who have been validated as being U.S. citizens.

Track and Monitor Access to Network Resources and Cardholder Data

The platform maintains comprehensive logs and records, enabling organizations to track and monitor user activities, data access, and file transfers. Real-time monitoring capabilities allow administrators to promptly identify and respond to potential security incidents or unauthorized access attempts. Kiteworks features a built-in audit log, capturing all user actions for compliance reporting and security incident investigations. The CISO Dashboard provides a centralized view of the organization's security posture, facilitating risk identification and mitigation. It provides continuous, comprehensive feeds to SIEM systems via audit logs and the Splunk Forwarder. By leveraging these features, Kiteworks ensures a secure environment for sharing and collaborating on content while meeting PCI requirements for tracking and monitoring access to network resources and sensitive cardholder data.

Regularly Test Security Systems and Processes

The platform undergoes thorough yearly audits to verify the proper execution of controls. State-of-the-art penetration tests are conducted for internet-facing vulnerabilities, along with onsite tests for vendor corporate network vulnerabilities. These tests effectively identify and address potential security risks, ensuring a secure and compliant platform. Kiteworks also submits monthly reports to validate secure configuration adherence and resolution of incidents following documented processes. With these robust security practices, Kiteworks provides organizations with peace of mind, offering a secure environment that meets PCI requirements for secure systems and applications.

Maintain a Policy That Addresses Information Security for All Personnel

Kiteworks develops and maintains comprehensive security policies and procedures that require regular training and signoff by all personnel, which in turn helps ensure customer systems properly protect credit card data. Software developers are trained in and required to follow a secure software development life cycle (SDLC) process based on standards such as OWASP that protects the software supply chain, ensures secure coding practices are followed, and provides layers of security testing, internal scans for vulnerable libraries, third-party penetration testing, and both black box and white box bounty programs. Support personnel are trained in and required to follow rigorous security procedures when accessing customer systems or managing Kiteworks-hosted systems, to mitigate insider threats.

In conclusion, the heightened security, comprehensive data management features, and robust support for PCI DSS compliance offered by Kiteworks position it as a powerful ally for organizations that process, store, or transmit cardholder data. The numerous features—from firewall protection and password security, through to encryption standards, antivirus deployment, access privileges, unique user identification, physical access restriction, monitoring and tracking, regular testing of security systems, and a stringent information security policy—are indicative of the value Kiteworks provides in terms of a secure, compliant, and efficient environment for sensitive data management. As we navigate an increasingly digital age, with cardholder data security at the forefront of risk mitigation and customer trust, Kiteworks stands as a testament to the potential for a secure yet flexible data management platform. Harnessing the power of Kiteworks for your organization not only enhances your compliance with stringent PCI DSS requirements but also offers significant strategic advantages—fostering trust, securing customer loyalty, mitigating legal and financial risks, and enhancing your brand's reputation for data security. Embrace Kiteworks, and empower your organization to navigate the complexities of PCI compliance with confidence and ease.