Kiteworks

COMPLIANCE BRIEF

Enhancing Compliance and Security for Criminal Justice Information

Leveraging Kiteworks' Advanced Features to Ensure CJIS Compliance and Safeguard Sensitive Data

Kiteworks & CJIS

The Criminal Justice Information Services (CJIS) Division of the U.S. Federal Bureau of Investigation (FBI) manages and provides state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI), such as fingerprint records and criminal histories. Given the sensitivity of this information, U.S. law enforcement and other government agencies must ensure that their use of cloud storage services for the transmission, storage, or processing of CJI complies with the CJIS Security Policy, which establishes minimum security requirements and controls to safeguard CJI. The CJIS Security Policy integrates presidential and FBI directives, federal laws, the criminal justice community's Advisory Policy Board decisions, and guidance from the National Institute of Standards and Technology (NIST). The Security Policy defines 13 areas that private contractors, such as cloud service providers, must evaluate to determine if cloud services can be used consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for FedRAMP, a program under which Kiteworks has earned Moderate Authorization six years in a row. As such, Kiteworks can support companies with CJIS compliance in the following ways:

Incident Response

Anomaly detection provides organizations with immediate insight into unauthorized access attempts. By utilizing advanced AI technology, suspicious events such as potential data exfiltration are detected, triggering alerts through email notifications and audit logs. This enables organizations to promptly identify and respond to attacks, ensuring that all evidence is preserved for analysis, containment, recovery, and user responses. With these capabilities, Kiteworks helps organizations comply with the CJIS standards by facilitating efficient mandatory reporting of any data violations in a timely manner.

Auditing & Accountability

Kiteworks provides robust auditing and accountability features to ensure compliance and secure sensitive information. The platform maintains detailed logs and records of data access, transfers, and user activities, ensuring transparency and accountability. Real-time monitoring identifies and reports potential breaches promptly. Granular access controls enforce permissions and roles, reducing unauthorized access risks.

Solution Highlights

- Anomaly Detection and Real-time Monitoring
- Comprehensive Audit Logging and Reporting
- Role-based Access Control
- Content and User-based Policy Enforcement
- Multi-factor Authentication
- Integration With Security Information and Event Management (SIEM) Systems
- Comprehensive Mobile Security

Customizable reporting options generate detailed reports for audits, compliance assessments, and investigations. Kiteworks safeguards sensitive information across third-party communication channels, supporting organizations in maintaining security and compliance.

Access Control

Kiteworks provides granular access controls to secure sensitive information, including secure storage, role-based policies, secure email and shared folders, built-in audit logging, and a CISO Dashboard for monitoring and managing access controls effectively. These features ensure that only authorized individuals have appropriate access to sensitive information, protecting it from unauthorized access and potential data breaches.

Identification & Authentication

Administrators can set policies for password complexity, geofencing, and domain whitelisting and blacklisting, and enforce password changes during login. They can also apply granular multi-factor authentication and SSO policies by role and location utilizing RADIUS, SAML 2.0, Kerberos, authenticator apps, PIV/CAC, SMS, and more. These features enable organizations to detect and respond to security incidents, manage vulnerabilities, and maintain compliance with CJIS requirements.

Configuration Management

Kiteworks offers full administrative control over configuration management as well as access restrictions for changes. All changes are recorded in real time in the audit log and custom reports can be set up to track and report on these changes. Kiteworks' security features like multi-factor authentication and a hardened virtual appliance ensure the sensitive content related to these changes stays protected from unauthorized access.

System & Communications Protection & Information Integrity

The Kiteworks Private Content Network (PCN) provides a single point of integration that allows organizations to get the most out of their current security investments. Apply SSO, LDAP, AV, ATP, and DLP centrally to every exchange of sensitive information entering and leaving an organization. Plus, with end-to-end encryption and organizations owning their own keys, organizations can trust that they are in charge of their own email and file data.

Mobile Devices

Kiteworks offers comprehensive mobile security features, including encrypted file storage, whitelisted app control, remote wipe functionality, biometric authentication, view-only watermarked images, device agnosticism, and secure offline access. Files downloaded for offline use are stored in encrypted states on mobile devices, with encryption keys stored securely. The "Open in" functionality is controlled by a whitelisted app bundle, ensuring only approved apps can access Kiteworks files. Remote wipe allows administrators to remove account-specific data from a device as a security measure. Biometric authentication, such as facial or fingerprint recognition, adds an extra layer of security. These features enhance mobile security and protect sensitive information on the go.

By leveraging advanced capabilities, Kiteworks enables organizations to meet CJIS requirements and safeguard sensitive criminal justice information (CJI). With features such as anomaly detection, auditing and accountability, granular access controls, robust identification and authentication mechanisms, configuration management controls, system and communications protection, and mobile device security, Kiteworks empowers organizations to detect and respond to security incidents, maintain data integrity, and protect sensitive information across third-party communication channels. By ensuring compliance with CJIS standards, Kiteworks helps organizations in the criminal justice sector enhance their security posture and maintain the confidentiality, integrity, and availability of critical criminal justice information.