

White Paper: Enhancing CJIS Compliance with FileSure Defend

Introduction

The Criminal Justice Information Services (CJIS) Security Policy sets the minimum security requirements for access, storage, and transmission of Criminal Justice Information (CJI). Law enforcement agencies, contractors, and organizations that handle this sensitive information are required to implement stringent security measures to protect it from unauthorized access or breaches.

FileSure Defend is a powerful file auditing and access control solution that provides robust protections for CJIS compliance. By operating outside of the Windows security model, FileSure enforces explicit file access rules, monitors and records all file interactions, and prevents unauthorized operations—even by administrators. This white paper outlines how FileSure Defend helps organizations meet critical CJIS compliance requirements while enhancing the overall security of CJI.

CJIS Security Policy Overview

The CJIS Security Policy provides comprehensive guidelines to ensure the confidentiality, integrity, and availability of CJI. The key areas addressed by the CJIS Security Policy include:

1. **Access Control**
2. **Audit Logging and Accountability**
3. **Incident Response**
4. **Data Encryption**
5. **Secure File Transfer**
6. **Personnel Security**
7. **Physical Security**

Organizations must implement strict controls over who can access CJI, maintain detailed audit logs, and ensure that systems storing CJI are resilient against data breaches and cyberattacks.

How FileSure Defend Supports CJIS Compliance

FileSure Defend offers several features that directly address key areas of CJIS Security Policy, ensuring that your organization meets regulatory requirements and maintains the highest level of data protection for CJJ.

1. Access Control (Section 5.5)

CJIS mandates strict control over access to CJJ, requiring agencies to implement least privilege access and multi-factor authentication (MFA) to limit unauthorized access to sensitive data.

FileSure Defend's Role:

- **Granular Access Control:** FileSure Defend allows administrators to create detailed, rule-based policies for file access that operate independently of Windows ACLs (Access Control Lists). This ensures that only authorized personnel can access or modify CJJ, even if they have administrative privileges on the system.
 - **Administrative Control:** FileSure provides detailed control over administrative access, blocking unauthorized file operations even if an administrator attempts to perform them. This ensures that even those with elevated privileges are subject to security rules defined within FileSure.
-

2. Audit Logging and Accountability (Section 5.4)

CJIS requires comprehensive audit logging to ensure that all access to CJJ is recorded and available for review. Logs must be protected from tampering and retained for a minimum period, with real-time alerts for suspicious activity.

FileSure Defend's Role:

- **Tamper-Proof Audit Logs:** FileSure Defend records every file access attempt—whether successful or failed—and stores these logs in a tamper-proof system. These audit logs provide a comprehensive record of all activity related to CJJ and can be securely stored for compliance with CJIS retention requirements.
 - **Real-Time Monitoring:** FileSure provides real-time alerts on any unauthorized or suspicious file access attempts, allowing organizations to detect and respond to potential security incidents immediately.
-

3. Incident Response (Section 5.3)

CJIS mandates that organizations have a formal incident response plan in place to detect, report, and mitigate security incidents involving CJJ.

FileSure Defend's Role:

- **Breach Prevention and Detection:** FileSure can actively prevent unauthorized access to CJJ by blocking file operations based on predefined rules. This capability helps prevent breaches before they occur. In addition, FileSure generates alerts in real-time if a potential breach is detected, enabling rapid response.
 - **Detailed Forensics:** In the event of a security incident, FileSure's comprehensive audit logs provide the data needed for forensic investigations, ensuring that the root cause of the incident can be identified and addressed.
-

4. Data Encryption (Section 5.10)

To comply with CJIS, organizations must encrypt CJJ in transit and at rest to protect it from unauthorized access or interception.

FileSure Defend's Role:

- **Encryption Integration:** While FileSure focuses primarily on access control and auditing, it integrates seamlessly with encryption technologies that organizations use to secure CJJ. FileSure ensures that only authorized users can decrypt and access sensitive data, enhancing encryption-based protections.
-

5. Secure File Transfer (Section 5.6)

CJIS Security Policy requires that organizations securely transfer CJJ over networks and between systems.

FileSure Defend's Role:

- **Controlled Access to Files for Transfer:** FileSure Defend ensures that files containing CJJ can only be transferred by authorized users, reducing the risk of unauthorized sharing or accidental exposure during file transfers.
 - **Monitoring File Transfers:** FileSure can log all access to files before and after transfers, providing a comprehensive record of who handled the CJJ during transit.
-

6. Personnel Security (Section 5.1)

CJIS requires that only personnel with the appropriate background checks and security clearance are allowed access to CJI.

FileSure Defend's Role:

- **Customizable Access Policies:** FileSure Defend allows administrators to enforce customizable access policies based on roles, ensuring that only cleared personnel have access to files containing CJI. This reduces the risk of insider threats and accidental access by unauthorized employees.
 - **Audit User Activity:** FileSure tracks all user activity in relation to CJI, providing detailed insight into how users interact with sensitive information. This visibility allows organizations to detect and investigate improper access attempts or misuse by employees.
-

7. Protection of Audit Logs (Section 5.8)

Protecting audit logs from unauthorized access and modification is essential to maintaining their integrity.

FileSure Defend's Role:

- **Log Integrity and Protection:** FileSure's self-auditing feature ensures that audit logs are protected from unauthorized access or tampering. Access to the FileSure console and the logs themselves can be tightly controlled through FileSure's own rules model, ensuring that only authorized personnel can view or modify logs.
 - **Audit Log Retention:** FileSure ensures that audit logs are retained according to CJIS requirements, providing agencies with a long-term record of file access activities to support audits and investigations.
-

FileSure Defend: Operating Outside the Windows Security Model

One of the unique advantages of FileSure Defend is that it operates independently of the Windows security model. This means that it can block file operations that would otherwise be allowed under standard Windows permissions. Even administrators cannot bypass FileSure's rules, making it an ideal solution for preventing ransomware, malware, or unauthorized actions that could compromise CJI. By working outside the Windows ecosystem, FileSure offers a higher level of security and protection that can prevent threats, even from high-privileged users.

Conclusion

CJIS compliance is essential for any organization handling Criminal Justice Information, and failure to comply can result in legal penalties, security breaches, and loss of trust. FileSure Defend provides a powerful, comprehensive solution for CJIS compliance, ensuring that sensitive CJI is protected at every level—from access control and audit logging to incident response and file transfer security.

With FileSure Defend, organizations can achieve CJIS compliance while improving overall file security, minimizing insider threats, and preventing unauthorized access, even from system administrators.

For more information on how FileSure Defend can assist with CJIS compliance, contact us today.