Simplify CJIS Data Security Compliance with the BrickStor Security Platform

All IT Departments Must Adequately Protect CJI Data

Criminal Justice Information Services (CJIS)[1] , the largest division of the Federal Bureau of Investigation (FBI), establishes and enforces security and policy standards for the handling, access, and dissemination of criminal justice information. These standards are crucial to ensuring the confidentiality, integrity, and availability of sensitive law enforcement data. CJIS security policies cover various aspects of information security, including access controls, encryption, physical security, auditing, and incident response.

Demonstrate Data Security and Compliance with CJIS

Entities that handle Criminal Justice Information (CJI) are required to adhere to CJIS security policies to safeguard sensitive data and maintain the trust and integrity of the criminal justice system. The BrickStor Security Platform makes it easy for non-cybersecurity specialists to maintain appropriate security controls at all times to both ensure and demonstrate continuous compliance to security teams and auditors.

BrickStor Addresses Data Related CJIS Security Requirements and Controls Out of the Box

Access Controls:

- **Implement strong authentication**

  BrickStor SP provides strong access control features and integration with Active Directory and LDAP to ensure access is limited to authorized users. The BrickStor GUI supports multifactor authentication (MFA).

- **Enforce least privilege**

  BrickStor employs a zero trust architecture; by default no users or groups have access to data on the system. Users and groups must be explicitly granted access to data. BrickStor's patented active defense technology[2] alerts on unusual and inappropriate privileged access to thwart abuse or access through compromised accounts.

1. https://www.fbi.gov/services/cjis
2. Cybersecurity Active Defense in a Data Storage System, US 11,868,495 B2

- **Regularly review access permissions**

  Integrated compliance tools enable admins and data owners to review access control settings and modify or assert their correctness on a periodic basis.

- **Monitor and log access activities**

  BrickStor's user activity monitoring and analysis capabilities log permission changes and the details of each file operation including the time, account, file protocol, client IP, file operation, operation size, and full path. The GUI allows admins and security operators to investigate and review access activity. The zero trust architecture of BrickStor is constantly evaluating trust for each access activity. BrickStor's active defense uses built in artificial intelligence to automatically alert on suspicious activity and even block and isolate malicious activity to provide a real time response to aid in the organization's rapid response

Encryption:

- **Encrypt data at rest**

  BrickStor supports up to two levels of FIPS encryption for data at rest using AES-256 algorithms.

- **Use strong encryption for data transmission**

  BrickStor provides equally strong encryption for data in flight for file protocols and TLS connections.

- **Ensure proper key management**

  BrickStor SP employs key orchestration to manage keys and certificates within BrickStor. BrickStor can leverage its internal key manager with replication and backup features or connect to a KMIP compliant key server. BrickStor supports automatic key rotation.

Auditing and Logging:

- **Establish comprehensive logging**

  BrickStor SP provides a full audit log of events that can be retained on the system and/or sent to a log repository and System Issue Event Manager (SIEM).

- **Regularly review and analyze logs**

  BrickStor provides a GUI to review, analyze, and investigate logs for anomalous and malicious behavior.

- **Retain logs as per CJIS policies**

  BrickStor enables the retention of logs in an immutable format. The organization can manage retention polices to enforce both a minimum and maximum retention time.

Incident Response:

- **Report incidents promptly**

  The incident management workflow of BrickStor provides comprehensive reporting about incidents, the actions taken, and the current disposition. This information can be provided in real time to existing SOC systems via webhooks. With advanced information about data-oriented incidents stakeholders and management can provide accurate information and execute informed decisions.