RACKTOP

CUI Cyberstorage Solution

BrickStor SP Addresses NIST 800-171 Data Controls with Ease

Control 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

- BrickStor SP's Microsoft Active Directory and LDAP integration with security groups enables compliance with ease. Data owners and admins can review and modify access control through BrickStor SP's integrated compliance tools.

Control 3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

- BrickStor SP provides role-based access control and a full audit of admin and user activities on the system.

Control 3.1.21 Limit use of organizational portable storage devices on external information systems.

- BrickStor SP offers an easy method for providing authorized access to data from a central protected location. BrickStor SP can be used for Virtual Desktop Infrastructure (VDI), as well as a file sync and share repository, negating the need for users to use portable storage devices, such as USB drives.

Control 3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

- 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).

Control 3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

- Granular auditing on a per user and per transaction basis provides full accountability and can be used for forensic investigations and prosecution.

Control 3.3.7 Provides an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

- BrickStor SP maintains timing synchronization with network time protocol (NTP), ensuring logs use the correct time stamp.

Control 3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.

- BrickStor SP provides logs that can be replicated automatically along with taking immutable snapshots to prevent tampering. The system can also send these logs to a SIEM.

Control 3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

- BrickStor SP maintains serial numbers and firmware versions for all components in a database and can ensure original authentic parts through a secure supply chain.

Control 3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

- All BrickStor SP drives are FIPS certified self-encrypting drives that are capable of cryptographic erasure for media sanitization compliant with NIST SP 800-88 Revision 1.

Control 3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

- BrickStor SP protects all data at rest and replicated data in transit with encryption. All drives use inline AES-256 encryption with zero impact to performance. The system can encrypt data with a second method of AES-256 encryption for extra protection.

Control 3.8.2 Limit access to CUI on information system media to authorized users.

- BrickStor SP provides strong access control features and integration with Active Directory to ensure access is limited to authorized users. Compliance tools enable users and data owners to review file access and access control settings.

Control 3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.

- All BrickStor SP drives are Seagate TAA/BAA FIPS certified self-encrypting drives that are capable of cryptographic erasure for media sanitization compliant with NIST SP 800-88 Revision 1.

Control 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

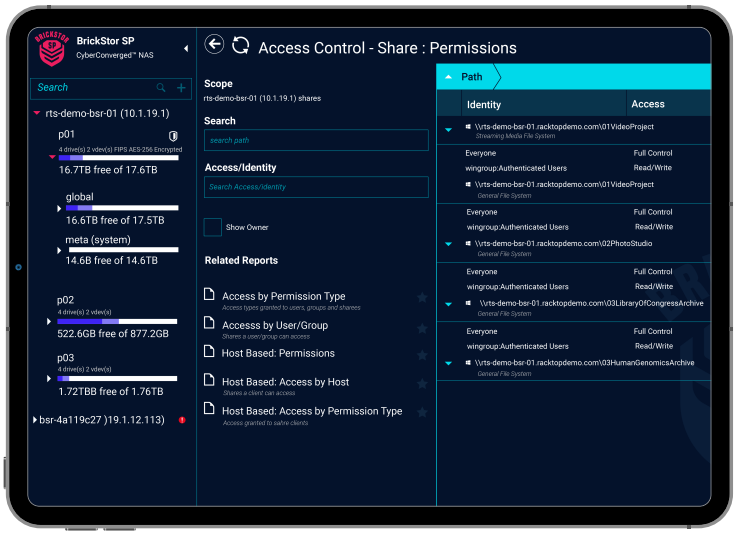
- BrickStor SP supports two distinct layers of AES-256 encryption by employing encryption at the file system and the drive level. All BrickStor drives are Seagate FIPS 140-2 certified self-encrypting drives. Disks and SSDs can be safely transported without risk of data exposure or compromise.

Control 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

- Data replication between BrickStor SP platforms is always encrypted and protected. Encryption and digital signatures at the file protocol level enables further protection between the data repository and the user.

Control 3.13.10 Establish and manage cryptographic keys for cryptography employed in the information system.

- BrickStor SP employs key orchestration to manage keys and certificates within BrickStor and other divergent information systems.



Access control

Control 3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

- BrickStor SP uses FIPS 140-2 level 2 validated cryptography.

Control 3.13.16 Protect the confidentiality of CUI at rest.

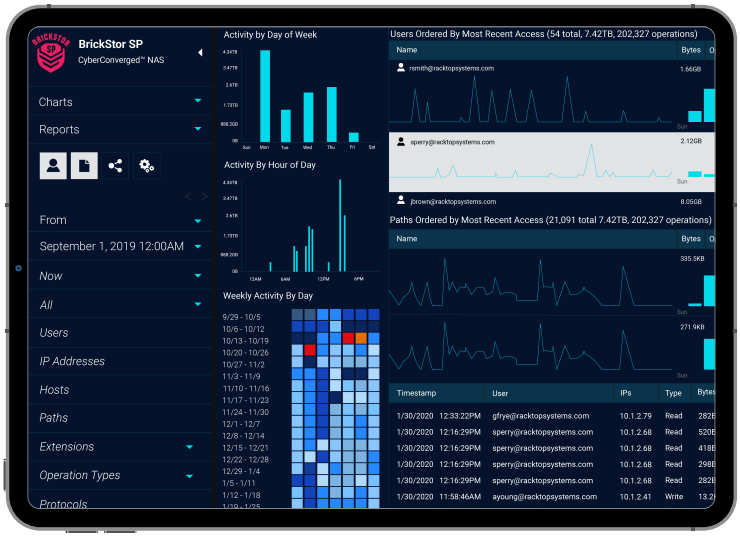
- BrickStor SP protects all data at rest through access control, user permissions, and FIPS 140-2 validated encryption.

Control 3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.

- BrickStor SP's automatic malware and ransomware protection enables organizations to roll back to a pre-infected version. User Behavior Auditing and strict access control prevent the spread of malware.

Control 3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

- BrickStor SP provides the ability to monitor actions and discover anomalies in user or application interactions with system data. Built in User Behavior Auditing and Analysis captures the source IP, file operation, and user identity of each file operation. This enables users or systems to immediately terminate access to prevent and stop attacks and insider threats before it is too late.



User behavior auditing