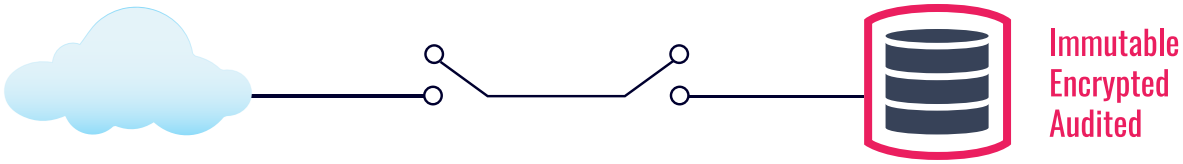
RACKTOP

DoD Strength Air Gap Data Protection

As threats to organizational data continue to evolve and become more sophisticated, the only way to protect your most critical data is to remove it from the network completely. But with the volume of new data growing exponentially, it's impractical to implement a disconnected solution which is both secure and efficient. Tapes and portable disks are prone to theft and data loss, and backup systems with discretionary access controls are easily circumvented by rogue insiders or advanced persistent threats. To truly protect your most critical data at scale, an automated air gap architecture is the most secure and scalable solution.

Every organization has the right to protect their data as if it were a national secret. That's why we built BrickStor SP using DoD principles for security and data protection. Not only will our technology protect you from long-term reliability issues like bit rot and file corruption, but you'll also stay safe from the hardest to detect cyber attacks including Insider Threats, Remote Access Trojans, and Ransomware Encryption and Exfiltration.



Protection of Primary Data Copy (Active Data)

- Data Protection Policies automatically create immutable encrypted snapshots
- User Behavior Analytics can alert on and mitigate suspicious behavior
- Administrative activity is audited and tied to change control tickets
- Administrative functions can only be performed from specific networks and hosts

Protection of Backup Copies (Air Gap)

- Leave data disks in a cryptographically locked state until they need to be unlocked and brought online to receive data. Drives are inaccessible even to an administrator without the drive encryption unlock keys present. Keys can be kept in another location and withheld until approved by a second person or process and the primary data is confirmed safe and available.
- Replicate encrypted copies of snapshots without the keys so the data cannot be mounted or accessed on the secondary BrickStor SP
- Create temporarily available network connectivity between the primary BrickStor SPs and secondary BrickStor SPs.
- Create a double hop and keep two backup copies of primary data. Have the primary system replicate to a secondary system and then have the secondary system replicate to a third system while always keeping the data encrypted.
- Administrative functions can only be performed from specific networks and hosts

Audit Trail

- All user and administrative actions are fully audited
- Searchable logs an exportable reports prove continuous compliance
- Forward audit data in real-time to 3rd party analysis systems

RackTop's unified approach to data security makes it easy to protect your organization's data from threats. Leverage BrickStor SP to securely meet the demands of any compliance regime.