Cyberstorage for Healthcare

BrickStor SP actively defends unstructured data from cyber threats with early detection

“Ransomware attacks are extremely costly in healthcare due to the long period of downtime, and without access to medical records patient safety is put at risk”

- HIPAA Journal

RackTop’s BrickStor Security Platform is the only software defined primary data storage solution that can actively defend an organization’s files from the most severe cyber threats and take active measures to stop ransomware, data theft, and malicious insiders in real time.

Today’s threat landscape demands that organizations must actively protect unstructured data rather than rely on backup and disaster recovery. Recovery from ransomware attacks is unreliable and unpredictable – affecting not only your team’s productivity but the organization’s reputation.

Zero Trust Architecture

- Brickstor SP is a frictionless way to implement a data-centric zero trust architecture without specialized skills
- Gain security and compliance without sacrificing performance
- Easier to maintain than legacy storage and security bolt-ons

Flexible Deployment Options

BrickStor SP is software than can be deployed to protect and move data at the edge, the core, or in the cloud. It eliminates vendor lock-in by enabling organizations to leverage any suitable storage capacity for secure NAS.

Common Use Cases

- Secure PACS imagery
- Protect clinical research
- Leverage object storage securely
- Enable a hybrid cloud architecture

Benefits

Data Protection and Recovery

End to end data integrity checks with automated snapshot and replication policies ensure your primary and secondary data copies are intact and protected. In the event of an attack you can isolate infected client devices and disable compromised accounts. Quickly recover and investigate with built-in analytics that pinpoint when and where an attack started.

Availability and Performance

With a highly available architecture and no single point of failure, BrickStor SP provides uninterrupted access to critical data. Reduce diagnosis and image access times to improve patient care and operational efficiency without sacrificing security or compliance.

Regulatory Compliance and Reporting

Generate automated reports to demonstrate compliance for audits, investigations, legal holds, and regulations.

Confidentiality

Granular access controls, user behavior auditing, and active defense ensure the most sensitive data stays confidential and protects the brand of the organization.

Cyber Resiliency

Active defense capabilities enable your organization to contain an attack so your team can continue providing critical care and services.