RACKTOP

Cyberstorage for Healthcare

BrickStor SP actively defends patient data from cyber threats with early detection and response

"In 2024, 37% of healthcare organizations said it took more than a month to recover from an attack" - HIPAA Journal

BrickStor SP enables organizations to store and protect enterprise data anywhere – at the edge, core, or cloud. BrickStor SP is the only end-to-end Cyberstorage solution with active security to detect and stop live ransomware attacks, insider threats, and data breaches in real-time. The software allows users to stop ransomware before it has a chance to encrypt your data. In the event of a breach, users can instantly recover files that have been affected and produce audit-ready compliance reports.

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

Common Use Cases

- Secure medical imagery
- Protect clinical research
- Leverage object storage securely
- Enable a hybrid cloud architecture
- Vendor Neutral Archive (VNA)

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. Organizations can leverage their preferred storage capacity for secure NAS.

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.

"healthcare organizations paid an average of $2.57 million in recovery costs in 2024, up from $1.82 million in 2023." - HIPAA Journal