

PUBLIC SAFETY & DIGITAL EVIDENCE

Evidence your agency can still trust — even after an attack.

BrickStor SP stops ransomware inside the storage layer, before it reaches body-camera footage, case files, or 911 records — and proves with a tamper-proof log that nothing was altered.



Body-camera footage and case files are now a primary ransomware target for county and municipal networks.



CJIS requires a tamper-proof chain of custody — a log an attacker, or an admin, cannot quietly edit.



Most agencies run lean IT teams — up against threats built for enterprise security operations.

Four capabilities, one storage platform



Active Defense

Inline detection evaluates every read, write, and delete against behavioral models — halting attacks in the storage path in under a second.



Attribute-Based Access

One policy — by user, device, clearance, and context — enforced on every file operation across SMB, NFS, S3, and web access.



ImmutaVault

Immutable, virtually air-gapped recovery copies that survive even a compromised administrator account.



Bulk Remediation

Patented file-level recovery restores only the files an attack touched — thousands of files back in seconds, not a full restore.

PROVEN IN STATE & LOCAL GOVERNMENT

"With BrickStor SP, I'm more confident in my data than ever before — I can recover very easily."

Florida Keys Electric Cooperative • 33,000 utility customers protected

Built for law enforcement & public safety

- Protects 911 dispatch records, incident reports, evidence files, and body-camera footage at the storage layer, before an attack can spread.
- Preserves court records and case filings with an immutable, tamper-proof audit trail — the chain of custody holds even under attack.
- Restores only the files an incident touched, so dispatch and court systems come back on the timeline citizens expect — not days later.

FBI CJIS Security Policy v6.1 readiness

Jun 26, 2026

CJIS Security Policy v6.1 takes effect

Sep 21, 2026

FIPS 140-2 validated modules sunset

Sep 30, 2027

Formal enforcement period begins

CONTROL FAMILIES SUPPORTED

Access Control (AC/IA)

Audit & Accountability (AU)

System & Comms Protection (SC)

Contingency Planning (CP)

System Integrity (SI)

ALSO ALIGNS WITH

NIST CSF

StateRAMP

CIS Controls

HIPAA

IRS Pub 1075

Platform specifications

Protocols	NFS, SMB, S3, and BrickStor Web Drive — served from a single dataset with full interoperability
Deployment	Physical appliance • SAN gateway (iSCSI / Fibre Channel) • virtual appliance (KVM, Hyper-V, ESXi, AWS, Azure, Google Cloud)
Encryption	AES-256, FIPS 140-3 validated, with integrated key management (HSM / KMIP)
Hardware partners	HPE, Crystal Group, Curtiss-Wright (appliance) • Pure Storage, HPE, IBM, JetStor (SAN gateway)
Audit trail	Immutable logs capture full user, session, and context detail for forensics and regulatory review

Procurement & onboarding

GSA Schedule

NASA SEWP V

Carahsoft State & Local

Hub Central

Centralized management across every BrickStor deployment in the agency, from one console.

Jumpstart Program

Guided onboarding built for the lean IT teams most agencies run with.