MINIO

Object-Native Ransomware Defense

“If credentials get compromised, AIStor encryption still protects the data. That extra layer matters in ransomware scenarios.”

— Platform Engineering Lead, Defense Contractor

Last line of defense. AIStor makes it immutable.

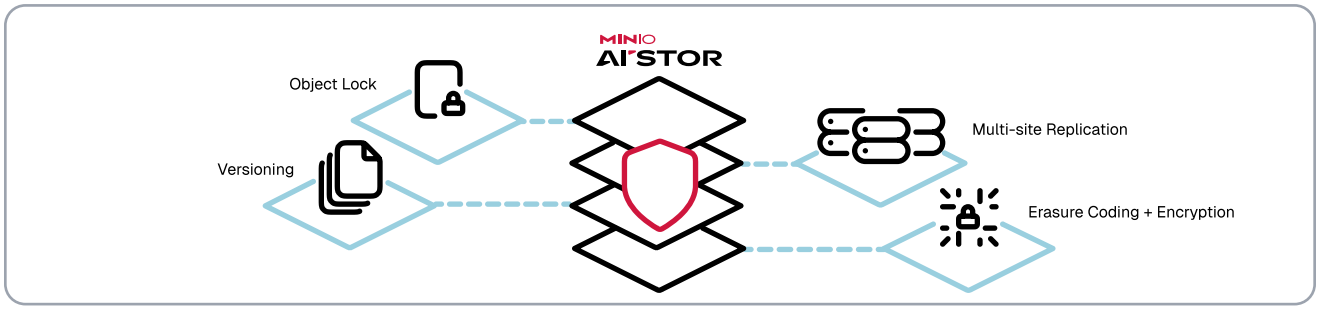
- **Ransomware protection at the storage layer:** The last line of defense when everything else fails
- **Immutability built in at write time:** Not bolted onto backup infrastructure
- **Compliance mode is absolute:** Locked objects can't be modified or deleted, even by admins
- **Every version is a full copy:** Restore without reconstruction
- **Deletes don't propagate:** Replicas stay clean automatically
- **Recovery in minutes, not days:** Surgical restore, not ransom negotiation

The Challenge: Backup Infrastructure Is a Target, Not a Safety Net

Backup servers sit on the same network as everything else, often with service accounts that have broad access because the software requires it. Attackers know this. Major backup platforms have all had CVEs exploited in the wild. Once attackers have a foothold, they dwell for days or weeks, map your environment, identify your backup infrastructure, and compromise it before they encrypt anything else. By the time ransomware detonates, your backups may already be gone. Even if they're not, restore tests that happen quarterly (if at all) don't tell you much when you need to recover everything at once. The catalog database that indexes your backups is itself a single point of failure. Replicas sync deletes alongside writes. The RPO you promised leadership assumes a recovery path that may not exist when you need it. The storage layer is the last line of defense, and most backup architectures don't treat it that way.

The AIStor Solution: Built-In Ransomware Defense

AIStor approaches ransomware differently than backup-based protection. Instead of creating recovery points you hope are still valid, it makes objects immutable at write time, preserves every version as a full copy, and replicates data without replicating deletes. Each capability works independently. Compromise one, the others still hold. Granular access controls let you scope permissions so applications can write new objects but can't modify or delete existing versions, limiting blast radius when credentials leak. Configure these capabilities together and you have layered protection that doesn't depend on detection speed or operational discipline.



Immutable Object Lock

Object Lock applies WORM (Write Once, Read Many) protection at the S3 API level. Set a retention period, and AIStor refuses all modification and deletion requests until it expires, regardless of who issues them.

Compliance mode is absolute. No user, no administrator, no root credential can alter or delete a locked object. The storage system enforces the policy. Humans cannot override it. This is fundamentally different from backup immutability that can be bypassed with the right credentials or by compromising the backup server itself.

Governance mode provides the same default protection with a controlled override for users holding specific bypass permissions. This is useful for development and staging environments where operational flexibility matters more than absolute immutability.

Legal Hold applies indefinite protection without an expiration clock. Objects remain locked until the hold is explicitly released, whether that's days, years, or decades. Use it for reference datasets, compliance archives, or any data where "unchangeable forever" is the requirement.

Retention state is tracked by the storage system itself. No external database to corrupt, no policy server to compromise. Ransomware that attempts to encrypt, rename, or delete locked objects fails completely.

Automatic Versioning

When versioning is enabled, every object write creates a new version with its own identifier, metadata, and erasure-coded shards. These are full copies, not deltas or diffs, so there's no reconstruction time and no corruption risk from incomplete chains.

An overwrite doesn't replace the previous version. It creates a new one. A delete doesn't remove data. It inserts a delete marker while previous versions remain intact. Malware that encrypts objects creates new encrypted versions. The clean originals remain untouched and recoverable.

Recovery is surgical. List versions, identify the last known good state, and restore. Production traffic continues uninterrupted. Combined with Object Lock, versions themselves become immutable. Attackers cannot delete the clean data they tried to destroy.

Multi-Site Replication

AIStor replication operates in write-only mode: new objects and versions replicate to remote sites, but delete operations do not. This is the critical difference from traditional replication. Write-only mode creates a one-way valve: data flows out, destruction doesn't flow back.

If ransomware compromises your primary site and issues mass deletes, your replica sites still hold every object the primary held before the attack. Credentials are site-scoped, so compromising one site's credentials doesn't touch the others. Failover to a clean replica, restore the primary, resume operations.

Replication happens in near real-time. Recovery point objectives measured in seconds, not the hours between backup windows.

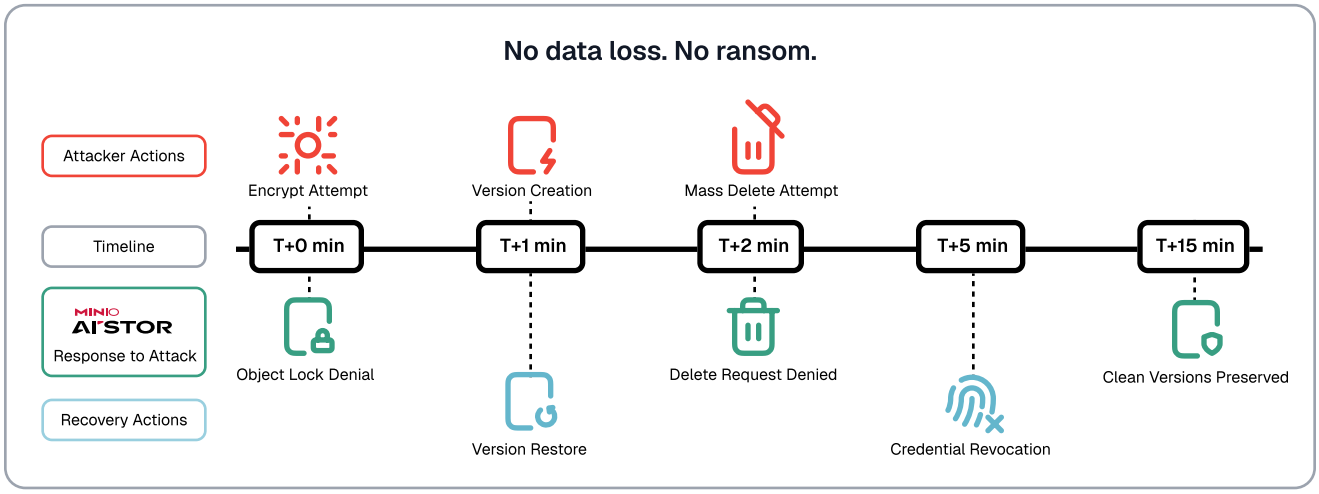
Data Durability and Privacy

Erasure coding distributes each object across multiple drives as data and parity shards. Lose drives during an attack, whether through hardware failure or malicious destruction, and the cluster reconstructs affected objects from surviving shards. No RAID controller to fail. No rebuild window during which data is vulnerable.

Encryption protects data at rest and in transit with keys you control. If attackers exfiltrate objects before encrypting, what they retrieve is ciphertext without the keys to decrypt it. Your data is unreadable outside your infrastructure.

What an Attack Looks Like Against AIStor

These protections work together. Here's what happens when ransomware meets AIStor:



T+0 minutes: Malware attempts to encrypt objects by overwriting them. Object Lock denies the operation. Originals unchanged.

T+1 minutes: Malware shifts tactics, writing new encrypted versions alongside originals. Versioning preserves every clean version as a full, independent copy. Clean data intact.

T+2 minutes: Malware attempts mass deletion. Compliance mode and Legal Hold deny all delete requests. Every denied request logged with timestamp, source IP, and credential identity.

T+5 minutes: Security team reviews inline audit logs. Mass delete denials are visible immediately. Compromised credentials identified and revoked. Blast radius contained by granular access policies that limited what those credentials could touch.

T+15 minutes: Operations restores affected objects to pre-attack versions. Cluster continues serving production traffic throughout.

Result: No data loss. No ransom. Minimal downtime. The attack becomes a ticket, not a crisis.

What Success Looks Like

The attack timeline above isn't theoretical. It's what organizations running AIStor experience when they've configured protection correctly and tested it before they needed it. After a ransomware event, the post-incident review should read: delete attempts denied by Object Lock (logged with timestamps and source IPs), clean versions identified and restored within 15 minutes, replica promotion tested and confirmed, production traffic uninterrupted during recovery. If you run quarterly DR tests and those tests include Object Lock validation, version rollback, and replica failover, the actual incident is just another test with higher stakes.

Why MinIO AIStor

AIStor delivers ransomware protection that doesn't depend on detection speed, backup windows, or operational discipline. Object Lock makes data immutable. Versioning preserves every state. Write-only replication maintains clean copies. Erasure coding survives hardware failures without RAID rebuild windows. Encryption keeps exfiltrated data unreadable. Access controls limit blast radius. Audit trails enable rapid response. Each layer works independently. Together, they close the gaps that backup-based protection leaves open.

For regulated industries, AIStor is the first S3-compatible platform Cohasset-assessed for SEC 17a-4(f), FINRA 4511(c), and CFTC 1.31(c)-(d) compliance alongside Amazon S3.

Ready to see it in action?

Visit min.io to learn more. Download AIStor and test it yourself. Request a demo to see how these protections work in your environment.