MINIO

Zero-Trust Identity & Access Management for Object Data

“We trust MinIO for mission-critical data storage, ensuring availability and scalability.”

Data Platform Engineer, Global Investment Bank

Every request verified.
Every action controlled.

- **Full S3 IAM compatibility:** Existing apps work without code changes
- **Native IDP integration:** Active Directory, Okta, Azure AD, and any OIDC provider
- **Your directory is the source of truth:** No duplicate identity silos
- **Granular policy control:** Scoped to bucket, prefix, or individual object
- **Deny-by-default:** Users only get what's explicitly granted
- **Temporary credentials via STS:** Auto-expire, no long-lived keys
- **Complete audit trail:** Every auth attempt, every policy decision, every outcome logged

The Challenge: Partial S3 IAM Compatibility Creates Full Security Gaps

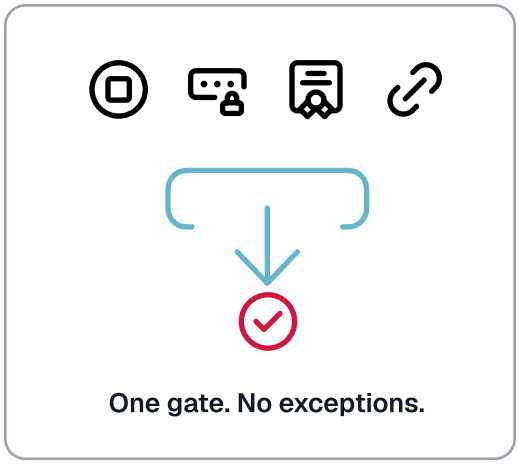
Most object storage platforms offer basic authentication with identity silos, IDP bottlenecks, limited S3 compatibility, and proprietary policy syntax. As data sprawls across clouds, regions, and regulatory boundaries, teams maintain duplicate user databases disconnected from corporate directories, permissions drift as service accounts accumulate access, and audit logs fragment across systems. The threat data makes this untenable. In 2025, credential theft became the leading attack vector: infostealer malware stole 1.8 billion credentials, stolen passwords factor into 86% of breaches at an average cost of $4.81 million per incident, and over half of ransomware victims had credentials exposed before the attack. Long lived credentials are the root cause. Static access keys leak into source code, CI/CD logs, and container images. They never expire. One weak identity link can cascade into reputational damage and regulatory fines. Organizations need temporary credentials that expire automatically, granular policies that enforce least privilege, native integration with corporate identity systems, and unified audit trails.

The AIStor Solution: Unified Access Control at the Data Layer

AIStor unifies application identity, corporate IDP integration, and granular policy controls at the storage layer. Unlike systems that rely on external API gateways or proxy-based identity enforcement, AIStor performs authentication and authorization directly at the storage layer. Security Token Service (STS) issues temporary credentials with AssumeRole and federated access built in, eliminating the long lived keys that drive most credential breaches. Direct connections to Active Directory, Okta, Azure AD, and SAML providers enable just in time provisioning and automatic group to policy mapping, so identity governance happens once, not across every system. Attribute based policies and role based access control give security teams precise control over who can access what data, scoped to bucket, prefix, or individual object.

Total Access Control, Native to the Data Layer

AIStor delivers complete access control for object data: application identity, corporate IDP integration, and granular policy controls in one platform.



AWS-Compatible IAM. Full S3 API compatibility with AWS STS for temporary credentials, AssumeRole for federated access, and native support for AWS Signatures V2/V4. Every request must prove identity before touching data, validated cryptographically through a single verification layer. JWT tokens and OIDC/OAuth for modern applications. Client X.509 certificates for service to service authentication. Presigned URLs for time limited sharing and explicit anonymous access for intentionally public resources. Developers continue using AWS SDKs without modification. STS issues credentials from 15 minutes to 365 days, each inheriting parent permissions and expiring automatically. Session policies restrict access further by IP range, time window, or resource scope. Drop in replacement for existing S3 workflows.

Enterprise IDP Integration. Connect directly to Active Directory, LDAP, Okta, Azure AD, Google Workspace, and any OIDC provider. Your corporate directory remains the single source of truth. Users authenticate with existing credentials. Group memberships map automatically to access policies. Just in time provisioning creates accounts on first login. Automatic directory sync purges credentials for removed users and updates policy assignments when roles change. Azure AD integration queries the Microsoft Graph API for group names rather than UUIDs. No duplicate databases. No sync jobs to maintain. Eliminates identity silos, reduces administrative burden, and strengthens governance.

Granular Policies. AWS IAM compatible JSON policies with the same syntax, structure, and evaluation logic. Policies codify real business rules: restrict analysts to read only access from corporate IP ranges, limit service accounts to specific buckets, require conditions for delete operations. Attach policies to users, groups, or service accounts. Least privilege access becomes enforceable and practical. Fine grained controls operate at bucket, prefix, and object level. Attribute based policies evaluate request context including source IP, time of day, and resource tags. Role based access control defines permission sets, read only, write, or full admin, that apply consistently across teams. Deny by default semantics ensure no access

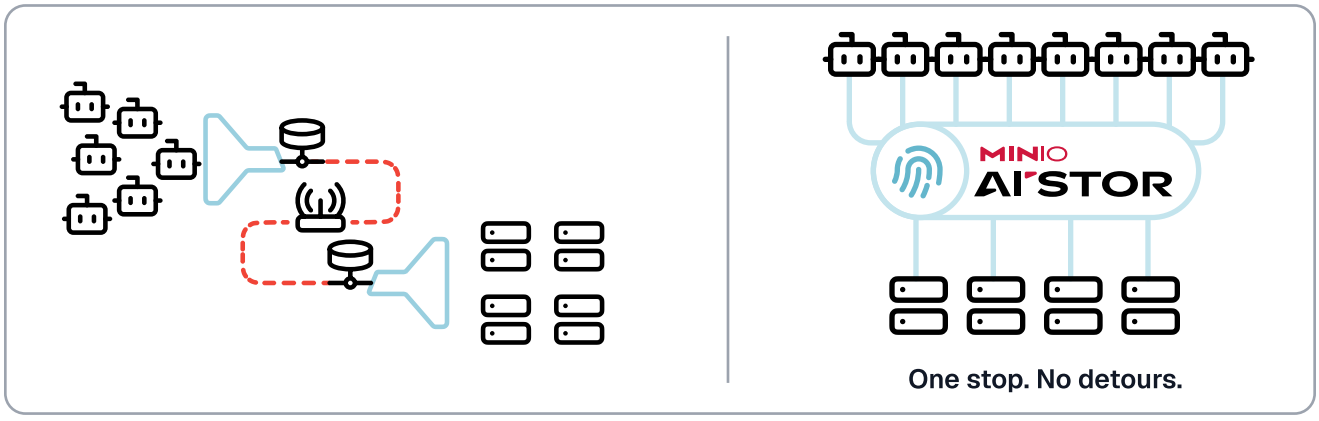
without explicit grant. Deny statements override allow. Users cannot exceed their most restrictive assigned permissions. The authorization engine evaluates every request in microseconds, even under millions of daily calls. No bottlenecks. No blind spots.

Built for Application Identity, Not Just Human Logins

Object storage IAM is fundamentally about application identity, not just human logins. Machine learning pipelines, data lakes, and analytics platforms need programmatic access scoped to specific data and operations. Portal based authentication designed for humans does not serve workloads that run continuously, scale dynamically, and span organizational boundaries.

AIStor delivers IAM at the storage layer with direct API access. Traditional architectures route identity decisions through external gateways or proxy services that sit between applications and data. Every request adds network hops, translation overhead, and a potential point of failure. When those gateways saturate under load, the entire data pipeline stalls. AIStor eliminates this by handling authentication and authorization natively, at the point where data lives. No proxy delays. No external dependencies in the request path. No bottleneck between your applications and your data.

Role switching supports cross account scenarios where workloads require access across teams, environments, or partner organizations. Real workloads demand specific access patterns. ML pipelines get read only access to training data and write access to model outputs. BI tools access specific datasets without visibility into adjacent data. Partner organizations access shared resources with time limited permissions and full audit visibility. Each pattern enforces least privilege by design, not as an afterthought.



Every Decision Logged, Every Action Auditable

Every authentication attempt and authorization decision generates a log entry with full context: who attempted access, to what resource, when, how they authenticated, the outcome, and why. Logs stream to Elasticsearch, Splunk, Kafka, or any external messaging service, creating an immutable audit trail.

This matters for compliance. SOC 2 auditors need evidence of access control enforcement. HIPAA requires audit trails for protected health information. PCI DSS demands proof that cardholder data access is logged and monitored. AIStor provides the raw material for all of these, generated automatically as a byproduct of normal operations. CISOs get defensible evidence of governance on demand.

This matters for incident response. When a breach occurs, security teams need to reconstruct events quickly. With AIStor audit logs, they can trace exactly which credentials accessed which objects, identify the scope of exposure, and establish timeline in minutes, not days.

For organizations using external policy engines, AIStor supports pluggable authorization. Open Policy Agent and similar systems integrate with AIStor's authorization flow while maintaining the same audit trail. Every verdict, allow or deny, is deterministic, logged, and explainable.

Why MinIO AIStor

AIStor delivers enterprise identity and access management without the complexity of bolt-on security layers. Zero trust by default—every request authenticated, every action authorized. Defense-in-depth architecture with multiple methods of identity proof, layered policy checks, and external control integration. Compliance you can prove through immutable audit logs and reporting on demand. Performance without trade-offs: sub-millisecond authorization decisions at hyperscale. Future-proof integration that works seamlessly with existing identity providers and adapts as new standards emerge. In an era where breaches begin with compromised credentials, AIStor ensures identity and access control are not afterthoughts—they are the foundation of your enterprise data security strategy.

Ready to see it in action?

Visit min.io to learn more. Download AIStor and try it yourself. And request to talk to our team about your environment, and see a demo. We'll show you what's possible.