THREADSYNC — MAGIC RUNTIME

Magic Runtime — Evaluation Checklist

February 2026 · v2.0 · magic.threadsync.io

Enterprise Evaluation

Everything you need to evaluate Magic Runtime for enterprise deployment

Security Model

Threat model, sandbox architecture, and hardening guide

View Security Docs

Release Verification

SHA256 checksums and verified downloads

View Releases

Contract Specification

Complete schema reference for controller contracts

View Spec

2-Week Evaluation Checklist

Week 1: Setup & Security Review

- [ ] **Deploy Production Stack**
  Follow Quick Start to deploy on test environment
- [ ] **Verify artifact checksums**
  Download SHA256SUMS and verify integrity
- [ ] **Review security model**
  Evaluate threat model against your requirements
- [ ] **Apply hardening checklist**
  Complete production hardening steps
- [ ] **Test health endpoints**
  Verify `/api/health` and `/api/readyz` return expected responses

Week 2: Functional & Integration Testing

- [ ] **Deploy demo controller**
  Execute included demo controller and verify contract enforcement
- [ ] **Create custom controller**
  Build a controller with your business logic and required capabilities
- [ ] **Test capability enforcement**
  Verify that undeclared capability usage is denied and logged

- [ ] **Review audit logs**
  Confirm capability usage and errors are logged with correlation IDs
- [ ] **Test resource limits**
  Verify timeout and memory limits are enforced correctly
- [ ] **Prometheus metrics**
  Connect to `/metrics` endpoint and verify expected metrics

Security FAQ

What does the sandbox isolate?

The sandbox contains: resource exhaustion (CPU/memory/disk), unauthorized database access, unauthorized network egress, secret exfiltration, filesystem persistence. See the threat model for full details.

Is it safe to run AI-generated code?

Magic is designed for first-party and AI-generated business logic within your organization. The capability model ensures code can only access explicitly declared resources. It is not designed for untrusted third-party code.

How are secrets protected?

Secrets are scoped per-controller. A controller can only access secrets explicitly declared in its contract. Cross-controller secret access is not possible. All secret access is audit-logged.

What authentication methods are supported?

API Key (X-API-Key header), JWT Bearer tokens, and mTLS. OIDC/SAML integration documentation is available for enterprise deployments.

How do I report security vulnerabilities?

Email security@threadsync.io. We acknowledge within 48 hours and follow coordinated disclosure practices. See disclosure policy.

Need Additional Security Materials?

Request security questionnaire responses, architecture diagrams, or schedule a security review call.

Contact Enterprise Team — enterprise@threadsync.io