The Startup Security Checklist

27 critical checks before your next audit or funding round

Section A - Access and Platform Foundations

- [ ] 1. Enforce MFA for all production and cloud admin accounts.
- [ ] 2. Lock down privileged roles with least-privilege access policies.
- [ ] 3. Rotate API keys and secrets at a defined cadence (<= 90 days).
- [ ] 4. Require SSO for internal tools handling customer or financial data.
- [ ] 5. Maintain an up-to-date asset inventory for services and data stores.
- [ ] 6. Tag systems by criticality and assign clear ownership per service.
- [ ] 7. Validate backup restore workflow quarterly, not just backup success.
- [ ] 8. Apply baseline hardening templates to servers and managed services.
- [ ] 9. Document trust boundaries and threat actors for core product flows.

Implementation note

Prioritize controls tied to customer trust, financial data, and privileged acc
ess paths first.

Section B - Application and Infrastructure Controls

- [ ] 10. Add authz checks at endpoint and business-rule layers.
- [ ] 11. Enforce strict input validation and canonicalization at API edge.
- [ ] 12. Add dependency vulnerability scanning to CI for every pull request.
- [ ] 13. Require branch protection and signed commits on protected branches.
- [ ] 14. Gate releases with automated SAST and secret detection scans.
- [ ] 15. Log security events with request correlation IDs and actor metadata.
- [ ] 16. Encrypt data in transit and at rest for all customer workloads.
- [ ] 17. Isolate high-risk workloads in separate network segments.
- [ ] 18. Define p95 and p99 performance budgets for critical transactions.

Implementation note

Integrate these checks directly into CI and release workflows to avoid one-tim
e security theater.

Section C - AI/Data Governance and Incident Readiness

- [ ] 19. Track model/data lineage if you use AI in product decisions.
- [ ] 20. Validate data retention and deletion policies against contracts.
- [ ] 21. Create a severity matrix with owner, SLA, and escalation path.
- [ ] 22. Run tabletop incident exercises at least twice per year.
- [ ] 23. Keep an evidence folder for audits (controls, logs, approvals).
- [ ] 24. Align security controls to SOC 2 or ISO 27001 readiness checklist.
- [ ] 25. Establish third-party risk reviews for critical vendor integrations.
- [ ] 26. Define a 30-60-90 day security improvement roadmap.
- [ ] 27. Review security KPIs monthly with engineering leadership.

Implementation note

Use this page to assign owners and target dates, then review status with leade
rship every month.