SkillForge

The Enterprise Marketplace for AI Agent Capabilities

Tagline: *"The App Store for AI Agents"*

Executive Summary

SkillForge is the definitive marketplace and runtime infrastructure for AI agent skills and capabilities. As AI agents become ubiquitous across enterprise software—from Apple's Xcode coding agents to autonomous customer service bots—organizations face a critical challenge: **how do you safely discover, deploy, and manage agent capabilities at scale?**

SkillForge solves this by creating a curated, secure marketplace where developers publish agent skills and enterprises subscribe to verified, compliant capabilities—with built-in runtime sandboxing, security scanning, and analytics.

Think: AWS Marketplace meets npm meets the App Store, purpose-built for the AI agent economy.

The Problem

The Agent Skills Crisis

1. **Fragmentation Hell**: Every AI platform has its own skill/tool format. OpenAI function calling differs from Anthropic's MCP, which differs from LangChain, which differs from custom implementations. Developers rebuild the same integrations repeatedly.
2. **Security Nightmare**: Agent skills execute code with user permissions. A malicious or buggy skill can exfiltrate data, make unauthorized API calls, or cause financial harm. There's no standardized security review process.
3. **Discovery Chaos**: Enterprises can't find quality agent capabilities. Open-source repos are unreliable. Internal builds are expensive. There's no trusted catalog.
4. **Compliance Vacuum**: Regulated industries (finance, healthcare, legal) need audit trails, version control, and compliance certifications for every capability their agents use. This infrastructure doesn't exist.
5. **No Monetization Layer**: Developers creating valuable agent skills have no way to monetize them. Enterprises have no way to pay for premium, supported capabilities.

Market Validation

- **AgentSkills.io trending on HN** (480 points, Feb 2026) — clear developer demand
- **Apple Xcode 26.3** just added native coding agent support — mainstream adoption imminent
- **Anthropic MCP ecosystem** growing rapidly — 1000+ community servers
- **Enterprise AI spending** projected at $500B by 2028, with agents as primary interface
- **Regulatory pressure** increasing (X/Grok investigations in UK/France)

The Solution

SkillForge Platform

1. Universal Skill Registry

- **One format, every platform**: Publish once, deploy to OpenAI, Anthropic, LangChain, AutoGPT, and custom frameworks
- **Semantic versioning**: Full version history with rollback capabilities
- **Dependency management**: Skills can depend on other skills; SkillForge resolves the graph
- **Documentation-first**: Auto-generated docs, examples, and playground

2. Security & Compliance Engine

- **Automated security scanning**: Static analysis, runtime behavior monitoring, permission auditing
- **Sandboxed execution**: Skills run in isolated environments with explicit capability grants
- **SOC 2 / HIPAA / PCI certification tracks**: For regulated industries
- **Audit logging**: Every skill invocation logged with full context for compliance

3. Enterprise Marketplace

- **Curated categories**: Sales, Support, Engineering, Legal, Finance, HR, Marketing
- **Verified publishers**: KYC for developers, enterprise verification for premium tiers
- **Usage-based billing**: Metered API calls with transparent pricing
- **Enterprise contracts**: Custom SLAs, dedicated support, on-prem deployment options

4. Developer Platform

- **SkillForge CLI**: `sf init`, `sf test`, `sf publish`, `sf analytics`
- **Local development sandbox**: Test skills against mock agents before publishing
- **Revenue dashboard**: Track installs, usage, revenue, user feedback
- **Skill templates**: Boilerplate for common patterns (API integrations, data processing, web scraping)

5. Runtime Infrastructure

- **Edge deployment**: Skills run close to agents for low latency
- **Auto-scaling**: Handle traffic spikes without developer intervention
- **Observability**: Tracing, metrics, logs for every skill execution
- **Failover**: Automatic fallback to cached responses when skills fail

---

Business Model

Revenue Streams

Stream	Mechanism	Target Margin
Marketplace Commission	20% of skill revenue (lower than App Store's 30%)	85% gross
Enterprise Subscriptions	$5K-50K/month for advanced features, SLAs, compliance	90% gross
Runtime Usage	$0.001-0.01 per skill invocation (metered)	70% gross
Certification Services	$10K-100K for SOC 2/HIPAA skill certification	80% gross
Professional Services	Custom skill development, integration support	50% gross

Pricing Tiers

Free Tier - 10,000 skill invocations/month - Community skills only - Basic analytics - Public skills only

Pro ($99/month) - 500,000 invocations/month - Premium marketplace access - Private skill hosting - Advanced analytics - Priority support

Enterprise ($5,000+/month) - Unlimited invocations - Custom SLAs (99.99% uptime) - On-prem deployment option - Compliance certifications - Dedicated success manager - Custom integrations

---

Market Size

TAM (Total Addressable Market)

$180B — Global enterprise software market transitioning to AI-native interfaces

SAM (Serviceable Addressable Market)

$45B — AI agent infrastructure and tooling spend by 2028

SOM (Serviceable Obtainable Market)

$2.5B — Agent capability marketplace and runtime (Year 5 target: 5% market share)

Market Timing

The window is NOW: - Apple just legitimized coding agents in Xcode (Feb 2026) - Every major tech company shipping agent features - No dominant marketplace exists yet - First-mover advantage is decisive in marketplaces

---

Competitive Landscape

Competitor	Positioning	SkillForge Advantage
LangChain Hub	Open-source chain sharing	No monetization, security, or enterprise features
OpenAI GPT Store	ChatGPT-only plugins	Locked to one platform; no enterprise focus
Anthropic MCP Registry	MCP server directory	Community-only; no runtime, billing, or compliance
AWS Bedrock Marketplace	Model marketplace	Models, not skills; Amazon lock-in
Hugging Face	Model hub	ML models, not agent capabilities

SkillForge's Moat: 1. **Cross-platform compatibility** — Not locked to any AI provider 2. **Enterprise-grade security** — Only platform with SOC 2 certified skills 3. **Developer economics** — Best revenue share drives skill creation 4. **Network effects** — More skills → more developers → more enterprises → more skills

---

Go-to-Market Strategy

Phase 1: Developer Community (Months 1-6)

- Launch free tier with 100 curated skills
- Partner with top open-source contributors (offer revenue share for porting)
- Sponsor AI/ML conferences and hackathons
- Build CLI tools and VS Code extension
- **Target:** 10,000 developers, 500 published skills

Phase 2: Startup Adoption (Months 6-12)

- Launch Pro tier
- Create "SkillForge Certified" badge for quality skills
- Case studies with early adopters
- Integration partnerships (Vercel, Supabase, Retool)
- **Target:** 1,000 paying customers, $500K ARR

Phase 3: Enterprise Expansion (Months 12-24)

- Launch Enterprise tier with compliance features
- SOC 2 Type II certification for platform
- HIPAA and PCI skill certification programs
- Enterprise sales team (5 AEs)
- **Target:** 50 enterprise customers, $5M ARR

Phase 4: Platform Dominance (Months 24-36)

- On-premises deployment for regulated industries
- Acquisition of complementary tools
- Geographic expansion (EU, APAC)
- **Target:** 500 enterprise customers, $50M ARR

Technology Stack

Core Platform

- **Runtime**: Deno-based sandboxed execution (leveraging Deno's security model)
- **API Gateway**: Custom Rust-based gateway for low-latency skill routing
- **Registry**: PostgreSQL + Redis for metadata, S3 for skill bundles
- **Search**: Elasticsearch for skill discovery
- **Analytics**: ClickHouse for high-volume invocation metrics

Security Infrastructure

- **Static Analysis**: Custom AST parser for dangerous patterns
- **Dynamic Analysis**: Runtime monitoring with syscall tracing
- **Secrets Management**: HashiCorp Vault integration
- **Encryption**: End-to-end encryption for skill inputs/outputs

Developer Experience

- **CLI**: Rust-based for speed, cross-platform
- **SDK**: TypeScript, Python, Go, Rust
- **Playground**: Web-based skill testing environment
- **Docs**: Auto-generated from skill schemas

Team Requirements

Founding Team (Pre-Seed)

- **CEO**: Enterprise SaaS background, GTM expertise
- **CTO**: Infrastructure/security experience (ex-AWS, Cloudflare, or similar)
- **Head of Product**: Developer tools background (ex-Stripe, Vercel, GitHub)

Key Hires (Seed)

- Security engineers (2)
- Platform engineers (3)
- Developer advocates (2)
- Enterprise sales (2)

Culture

- Developer-first mindset
- Security as a feature, not an afterthought
- Speed of execution
- Remote-first, async communication

Financial Projections

Metric	Year 1	Year 2	Year 3	Year 4	Year 5
Developers	10K	50K	200K	500K	1M
Published Skills	500	5K	25K	75K	200K
Enterprise Customers	10	100	500	1,500	5,000
ARR	$500K	$5M	$50M	$200M	$500M
Gross Margin	70%	75%	80%	82%	85%
Team Size	15	50	150	350	600

Funding Requirements

Round	Amount	Use of Funds	Timeline
Pre-Seed	$2M	MVP, founding team, initial skills	Q1 2026
Seed	$10M	Product expansion, initial GTM, enterprise features	Q4 2026
Series A	$40M	Scale GTM, international expansion	Q4 2027
Series B	$100M	Market dominance, acquisitions	Q4 2028

Risks & Mitigations

Risk	Probability	Impact	Mitigation
Platform lock-in by AI providers	Medium	High	Multi-platform support from day one; open standards advocacy
Security breach	Low	Critical	Defense in depth; bug bounty program; insurance
Slow enterprise adoption	Medium	Medium	Strong free tier drives bottom-up adoption

Risk	Probability	Impact	Mitigation
Competition from Big Tech	High	Medium	Speed, focus, and developer love beat slow incumbents
Regulatory changes	Medium	Medium	Early compliance investment; policy team

---

Why Now?

1. **Apple just legitimized agents**: Xcode 26.3 brings coding agents to millions of developers
2. **Regulation is coming**: The X/Grok investigations show governments are paying attention—compliance will be mandatory
3. **No incumbent**: The market leader position is wide open
4. **Developer demand**: AgentSkills.io trending proves the appetite exists
5. **Enterprise budgets unlocking**: AI spending shifting from experiments to production

---

The Ask

Raising $2M Pre-Seed to: - Build MVP platform and runtime - Curate initial 100 high-quality skills - Hire founding engineering team (5) - Establish developer community

Target Investors: - a]16z (AI infrastructure thesis) - Sequoia (developer tools track record) - Greylock (enterprise SaaS expertise) - Boldstart (dev-first investing)

Vision

In 5 years, every AI agent in the world runs on SkillForge-certified capabilities. We become the trust layer for the agent economy—the infrastructure that makes AI agents safe, reliable, and monetizable.

SkillForge: Where AI Agents Get Their Powers.

Generated by The Godfather | February 4, 2026