



CAPABILITIES STATEMENT

Worthify government technical services.

AI-enabled government technical services for secure software, data workflows, automation, cyber and systems analysis, and ReAgent-supported reverse engineering.

REQUEST PATH

Ask for a capabilities statement, staffing response, data-call support, proof-sprint discussion, or security review package.

REQUEST CAPABILITIES STATEMENT

DOWNLOAD PDF

BUYER QUICK FACTS

LAST VERIFIED 2026-06-12

LEGAL ENTITY

Worthify Inc.

VERIFIED 2026-06-12



WORTHIFY

EMAIL CONTACT

UEI

C73SKFSLN8A9

VERIFIED 2026-06-12

CAGE

11NJ7

VERIFIED 2026-06-12

SAM.GOV STATUS

active SAM.gov registration as of March 3, 2026

VERIFIED 2026-06-12

SAM RENEWAL SHOWN

2027-02-28

VERIFIED 2026-06-12

CORPORATE ADDRESS

3060 Williams Drive, Suite 300, Fairfax, VA 22031-4667

VERIFIED 2026-06-12

OFFICIAL SAM NAICS

Official SAM NAICS values are being confirmed before publication.

VERIFIED 2026-06-12

PROCUREMENT PATH

Available for program-fit conversations, capabilities statement requests, data-call support, and teaming or subcontract discussions.

VERIFIED 2026-06-12



SOURCE - ALIGNED OVERVIEW

Defense-cyber AI capability, written for a buyer screen.

Worthify Inc. builds practical automation for high-skill technical workflows in defense-cyber, reverse engineering, vulnerability research support, analyst augmentation, AI engineering, and government technical services.

The current product focus is ReAgent, an agentic AI platform for binary analysis, reverse engineering, vulnerability research support, and analyst workflow augmentation.

Worthify combines government contracting experience with applied AI engineering to help teams move from opaque software artifacts to validated findings, reports, and mission-ready technical output.

The operating model is services-to-product: support real mission work, learn from operational workflows, and turn that learning into repeatable software capability.

SERVICE AREAS

Services a buyer can map to staffing, delivery, or evaluation work.



Worthify provides engineers and delivery support for government programs that need secure software, data workflows, automation, cyber and systems analysis, and reviewable AI-assisted work products.

AI-fluent engineering support for program teams

Workflow automation, data pipelines, dashboards, and handoff artifacts

Technical evaluation support for model, deployment, and data-flow decisions

[VIEW SERVICE PAGE](#)

Technical Workforce Support

Embedded engineers can support software, evaluation, automation, documentation, and technical workflows inside existing teams.

AI / ML engineering and model-evaluation support

Secure software, Python automation, and integration work

Documentation and review notes tied to evidence a team can inspect

[VIEW SERVICE PAGE](#)

Government Software and Data Systems

Worthify builds secure applications, data pipelines, integrations, and automation around agency requirements, APIs, cloud boundaries, testing, and configuration baselines.

Data-call, reporting, and workflow automation support

Application and integration work with explicit requirements and tests

Architecture memos and handoff packages for review



Cyber, Systems, and Analysis

Worthify supports cloud, network, monitoring, reverse engineering, protocol review, and system assessment work where controls, evidence, and operational limits matter.

Reverse-engineering adjacent workflow support

Protocol review, system assessment, and technical analysis

ReAgent-assisted review patterns with human traceability

VIEW SERVICE PAGE

DETAILED CAPABILITY GROUPS

Product and services capabilities from the working statement.

Agentic Binary Analysis and Reverse Engineering

LLM-assisted disassembly and decompilation support

Function, string, global, cross-reference, and call-graph exploration

Dynamic function naming based on surrounding code and runtime context

Conversational workflows for querying binaries and analysis artifacts

Human-in-the-loop validation for analyst review, handoff, and confidence tracking



- Identification of security-relevant code paths and points of interest
- Patch-diff and version-difference analysis for security-relevant changes
- Pattern review for common bug classes and suspicious control or data-flow structures
- Assisted proof-of-concept development and reproducible technical reporting
- Workflow support from research and triage through productization and maintenance phases

Secure, On-Premise, and Sensitive-Data Workflows

- Offline LLM-agent workflows for sensitive binaries and controlled environments
- Air-gapped virtual machine analysis with network isolation
- Containerized or sandboxed tooling to reduce operational risk during live analysis
- Bring-your-own-knowledge workflows using internal documentation, prior cases, threat intelligence, and reference material

AI Engineering and Automation

- Applied generative AI and agentic workflow development
- Retrieval-augmented generation for internal knowledge and technical research
- Automation for repetitive analyst, reporting, and engineering tasks
- Rapid prototyping of AI-enabled tools for mission, product, and operational workflows

Government Contracting and Technical Services



WORTHIFY

EMAIL CONTACT

Subcontract execution and support for defense and government-adjacent technical programs

Technical staff augmentation in AI, data science, cyber, reverse engineering, and software engineering roles

Coordination with prime contractors, subcontract administrators, and technical points of contact

ENGAGEMENT PATHS

A first conversation should end in a clear next artifact.

Embedded AI / ML engineer

One or more technical contributors placed into an existing program or prime team for model, software, data, automation, or analysis work.

Delivery pod

A small Worthify-led team for a bounded workflow, prototype, data-call response, technical evaluation, or implementation package.

Workflow proof sprint

A 30-day benchmark-and-proof package for ReAgent or another AI-assisted workflow, with assumptions, results, and review notes separated from claims.

Technical evaluation support

Architecture review, data-flow review, model/deployment tradeoff analysis, secure-environment feasibility, and report packages.



WORTHIFY

[EMAIL CONTACT](#)

Capabilities mapping, staffing responses, data-call support, and government-services partner support without publishing confidential partner details.

BUYER OUTPUTS

- Staffed technical role or small delivery team
- Benchmark report or architecture memo
- Automation, dashboard, data pipeline, or evaluation artifact
- ReAgent workflow review with human-checkable notes
- Handoff package with assumptions, tests, constraints, and next steps

DIFFERENTIATORS

The useful distinction is controlled technical execution, not generic AI.

Defense-cyber focus

Worthify focuses on cybersecurity, reverse engineering, and technical analysis workflows where trust, reviewability, and operational constraints matter.

Product informed by mission work

The ReAgent roadmap is grounded in analyst workflow needs rather than generic AI-platform positioning.

Human-review discipline

Worthify treats AI as an analyst accelerator, not a replacement for technical judgment.



WORTHIFY

Controlled-environment design

[EMAIL CONTACT](#)

ReAgent is developed with sensitive binaries, air-gapped environments, and on-premise workflows in mind.

Operator-led execution

Worthify combines founder-led technical delivery with contracting, compliance, and capture activity.

TARGET CUSTOMERS AND PARTNERS

Good fit screens.

Defense and intelligence community contractors

Cybersecurity, product security, and application security teams

Reverse engineering, vulnerability research, malware triage, and incident response groups

Prime contractors seeking specialized AI, cyber, reverse engineering, or technical automation capability

Organizations that need analyst-facing AI tools deployable in controlled or offline environments

PUBLIC - SAFE EXPERIENCE

Subcontract and teaming experience with government-services primes. Worthify can discuss development, reverse-engineering adjacent workflow, staffing needs, and technical evaluation support while keeping partner, customer, contract-value, and clearance-count details sanitized unless approved for release.



WORTHIFY

EMAIL CONTACT



Review material should be scoped before sensitive artifacts move.

Do not send classified, CUI, export-controlled, or customer-sensitive material through public forms or email without an approved secure submission path.

Architecture diagram

Data-flow note

Trust-boundary summary

Customer-managed model placement notes

Access-control and audit-log discussion

Retention and deletion discussion

SBOM and supply-chain posture

Incident and vulnerability contact path



WORTHIFY

Official SAM NATCS values are being confirmed before publication.

EMAIL CONTACT

Prime, partner, customer, contract-value, and clearance-count details stay sanitized unless approved for public release.

Personal addresses, phone numbers, EIN, compensation records, and confidential attachments are not public-site material.

WORTHIFY

AI-enabled engineering services for government teams that need software, data, cyber, and technical analysis work they can review and hand off.

Worthify Inc. · UEI C73SKFSLN8A9 · CAGE 11NJ7

S I T E

Services

Capabilities

ReAgent

Procurement

Security

Method

Jobs

G E T I N T O U C H

Contact: contact@worthify.ai



6 **WORTHIFY**

AI-enabled government technical services with **EMAIL CONTACT** and hand off.