TRAVERGE

UNIFIED COMPLIANCE - SIMPLIFIED SECURITY™

WHY FRAAS

1. Fixed-fee annual contract. No staffing surprises.
2. FedRAMP Expert-led. No junior hand-offs ever.
3. Rev5 and 20x programs both fully supported
4. FedRAMP Class C-certified tooling included
5. Your team stays focused on your product.

FRaaS

FedRAMP-as-a-Service

Fully managed FedRAMP compliance for cloud service providers.
Fixed-fee. Expert-led. Compliant by design.

No matter your current FedRAMP posture, Traverge's FRaaS has the right fit.

40+
Years combined FedRAMP experience

12+
Years min per lead practitioner

60+
Initial and annual certification assessments lead

August 2026

SBA
U.S. Small Business Administration
SERVICE-DISABLED VETERAN-OWNED CERTIFIED

Why staff it when you can outsource it?

The practitioners you actually want are few and far between. If you can find them, you're competing against industry, government, and service providers for them. **FRaaS** gets you that expertise on a fixed-fee contract.

HIRING IN-HOUSE

- Six-figure salaries per head for senior FedRAMP expertise
- Months to recruit practitioners with real program depth
- Ongoing training, tooling, and management overhead
- Key-person risk when your one expert leaves
- Engineering and leadership time distraction

FRAAS BY TRAVERGE

- Fixed annual fee. No recruiting, no benefits, no surprises.
- Practitioners already FedRAMP qualified
- FedRAMP Class C (Moderate) certified operational tools
- Full team on your program. No single point of failure.
- Your engineering team stays focused on the product

GRC AUTOMATION

Documentation that stays current, automatically

Documentation drift is a silent compliance killer. Traverge pairs deep practitioner expertise with the industry's leading FedRAMP GRC platform.

- **Automated FedRAMP JSON/OSCAL Generation**

  Your System Security Plan and ConMon artifacts stay synchronized in real time. No manual document maintenance. No version drift. Full CR26 compliance out of the box.

- **Real-Time KSI Validation**

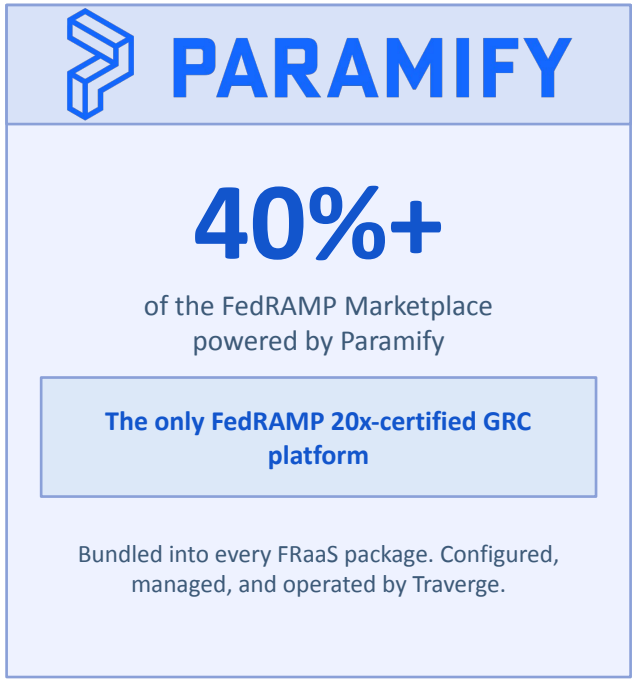
  Continuous validation against FedRAMP 20x Key Security Indicators. Automated evidence collection and machine-readable output for the FedRAMP PMO.

- **SSP and All Appendices**

  Traverge manages the complete FedRAMP documentation package, kept current and accurate as your environment evolves. No documentation sprints before assessment cycles.

- **Bring Your Own GRC**

  Already contracted with a GRC platform? Traverge manages your existing instance within the FRaaS scope without disrupting your current agreement or workflows.



Legacy: Not Ready for FedRAMP 20x? No Problem!

- **Full-Lifecycle Rev5 ConMon**

  Monthly scan analysis, SSP package management, POA&M lifecycle, and ConMon package delivery. Every deliverable, every deadline.

- **CR26 Compliance Included**

  CR26 hits Rev5 programs too. Rules such as new machine-readable formats, VDR and VER records, and a mandatory Trust Center. FRaaS covers every rule that applies.

- **All Five FRaaS Components Included**

  ITSM, Vulnerability Tracker, SCN Manager, Trust Center, and Paramify GRC all configured, managed for one fixed fee.

- **Agency Deliverables, On Time**

  PMO submissions, executive dashboards, and per-agency artifacts delivered on your ConMon cycle.

- **Clear Path to Dual**

  Ready to add 20x? FRaaS NextGen or Dual is a contract modification, not a new engagement.

LEGACY AT A GLANCE

- For Rev5 ATO holders
- Fixed annual fee
- JSON/OSCAL conversion in scope
- POA&M lifecycle managed
- Monthly ConMon packages
- Security and Privacy Impact Analysis
- Significant Change Management

NextGen: Pure FedRAMP 20x. Zero Legacy Overhead.

- **20x Initial Certification Support**

  End-to-end management from initial KSI evidence collection to final PMO submission.

- **KSI Continuous Validation**

  Real-time, machine-readable evidence generation across all CR26 Key Security Indicators.

- **Quarterly OCR Lifecycle**

  Full assembly and delivery of Ongoing Certification Reports to FedRAMP and target agencies every quarter.

- **All Five Components Included**

  Complete setup and management of ITSM, Vulnerability Tracker, SCN Manager, Trust Center, and Paramify GRC for one flat fee.

- **Certified Ecosystem & Trust Center**

  Operate within a fully FedRAMP-certified environment. This includes a FedRAMP-compliant Trust Center for securely sharing your Certification Data.

NEXTGEN AT A GLANCE

- Predictable fixed annual fee
- Managed by active FedRAMP SMEs
- FedRAMP-certified ecosystem
- Compliant Trust Center included
- Continuous KSI validation
- Automated quarterly reporting
- All FRaaS components included

Dual: Bridge Rev5 and 20x Under One Service.

- **Simultaneous Rev5 & 20x Management**

  Both certifications in parallel under one service. No coordination gap, no split accountability.

- **Turnkey CR26 Migration Built In**

  Full scope coverage for the CR26 transition. We convert your Rev5 program to official FedRAMP machine-readable standards alongside your active 20x rollout.

- **Strict 20x Operational Tempo**

  KSI telemetry reporting support, bi-weekly VDR scan support, continuous SDR updates, and quarterly OCR delivery with independent assessor attestation support.

- **Unified Tooling Architecture**

  All five core FRaaS components power both certifications at once, removing duplicate software fees and redundant administrative work.

- **Dual-Market Revenue Protection**

  Maintain active revenue from existing Rev5 agency customers while positioning your product for immediate adoption by agencies requiring 20x.

DUAL AT A GLANCE

- For multi-market providers
- Fixed annual fee
- Rev5 + 20x in parallel
- FedRAMP CR26 Ready
- Two FedRAMP Standards, One Solution
- Managed by Senior FedRAMP experts.

Custom: Your Framework. Your Tooling. Tailored Execution.

- **Scoped to Your Compliance Needs**

  Tailored support for mid-cycle starts, existing GRC platform integrations, partial coverage, or non-standard operational constraints.

- **Flexible Contracting Options**

  Choose between fixed-fee predictability or Time & Materials flexibility based on project scope, complexity, and internal resource alignment.

- **Broad Government Framework Support**

  Complete coverage across GovRAMP, CJIS, DoD SRG, and custom agency-specific ATO requirements.

- **Modular Tooling Selection**

  Select any combination of the five core FRaaS components so you pay only for the exact technical capabilities your program requires.

- **Proposal in Five Business Days**

  Share your current compliance posture and target framework to receive a detailed, fully scoped proposal within five business days.

CUSTOM AT A GLANCE

- Tailored scope for complex programs
- Fixed-fee or T&M pricing models
- Any federal or government framework
- Modular 5-component tooling stack
- Existing GRC platform integration
- Onboarding in as little as 30 days

Centralized ITSM Built for FedRAMP Governance.

- **Pre-Configured Operational Ticket Workflows**

  Built-in workflows out of the box for User Access (Add/Remove/Edit), Infrastructure Requests, Scheduled Maintenance, Feature Requests, and Bug Reporting.

- **Automated Security Incident Escalation**

  Dedicated Security Incident workflows auto-assign PAIN N-ratings and trigger mandatory 1-hour FedRAMP reporting windows for high-severity events.

- **Vulnerability SLA Tracking & Remediation**

  Vulnerability Management tickets auto-calculate remediation deadlines based on severity (N5 through N2) and route tasks directly to operational owners.

- **Integrated Change Management**

  Change Request tickets feed directly into the SCN Manager, providing complete audit trails for both standard modifications and emergency maintenance.

- **Centralized Compliance System of Record**

  Every operational task, maintenance window, and security event is logged in a single platform, giving assessors direct visibility into day-to-day operations.

ITSM AT A GLANCE

- 9 pre-configured ticket workflows
- Covers access, changes, and incidents
- Automated 1-hour incident escalation
- Built-in vulnerability SLA tracking
- Integrated SPIA and SCR management
- Centralized audit-ready evidence

End-to-End Vulnerability Tracking from Ingestion to Disposition.

- **Multi-Source Detection Pipeline**

  Pulls scanner findings, config drift, IaC diffs, pen test results, and SDR gaps into a single normalized pipeline, automatically generating assigned tracking tickets in your ITSM.

- **VDT and AVI Schema Enforcement**

  Enforces all required for active findings in the Vulnerability Detection Table and the required fields for accepted risks, automatically switching schemas based on finding state.

- **CR26 Dynamic SLA Engine**

  Calculates due dates using PAIN, IRV, and LEV metrics (N5=2d, N4=4d, N3=16d, N2=48d) to replace non-compliant static severity rules.

- **Real-Time CISA KEV Catalog Sync**

  Monitors live inventory against the CISA Known Exploited Vulnerabilities catalog, triggering instant security alerts and overriding standard SLA timelines when active exploits emerge.

- **Automated Lifecycle & Trust Center API Delivery**

  Unmitigated findings open past 192 days auto-convert to accepted status, feeding 14-day JSON API refreshes directly to your Trust Center.

VULN TRACKER AT A GLANCE

- Native ITSM ticketing integration
- VDT & AVI schema enforcement
- Dynamic CR26 PAIN matrix SLAs
- Real-time CISA KEV catalog sync
- 192-day auto-conversion engine
- 14-day Trust Center JSON API refresh

Defensible Change Management Built for FedRAMP CR26.

Automated SPIA Change Screening

Automatically classifies every system change into one of four CR26 categories: routine recurring, adaptive, transformative, or certification class change.

Automated Notification Timers

Enforces mandatory delivery windows, triggering 30-day advance alerts for transformative changes and 10-day post-completion notices for adaptive updates.

Strict 10-Field Template Enforcement

Mandates full completion of all 10 CR26-required data fields, ensuring assessor names, linked vulnerability records, and technical justifications are never omitted.

Immutable Audit Log Generation

Generates permanent, timestamped records for every change evaluation, capturing decision logic, change type, and evaluator identity for instant FedRAMP review.

Dual-Format Output & 12-Month History

Publishes a rolling 12-month change history in both human-readable and CR26-validated JSON formats for seamless Certification Data sharing.

SCN MANAGER AT A GLANCE

- Applies to Legacy, NextGen, Dual
- Automated CR26 change categorization
- 10-field notification enforcement
- Timers: automated, no manual tracking
- 12-month rolling history
- Dual-format: human-readable + JSON

FedRAMP-Compatible Trust Center Managed by Traverge.

- **FedRAMP-Compatible on GCP**

  Hosted at [client].traverge.com on GCP Zero Trust Architecture. Fully satisfies CR26 requirements without requiring a separately certified FedRAMP environment.

- **On-Demand Agency Access**

  Grants agencies immediate access to Certification Data via just-in-time provisioning (CDS-TRC-USH), completely isolated from your production systems.

- **Programmatic API Delivery**

  Exposes all Certification Data through machine-readable APIs (CDS-TRC-PAC), enabling automated fetches for JSON, Markdown, and PDF assets.

- **Complete Access Inventory & Logging**

  Tracks identity, timestamps, and requested resources per CDS-TRC rules, storing tamper-proof logs for 6 months for FedRAMP inspection.

- **Versioned Snapshots & Public Landing Page**

  Locks immutable snapshots to each OCR cycle for lifetime historical retention. Features a schema-validated landing page enforcing all 16 required fields.

TRUST CENTER AT A GLANCE

- Applies to Legacy, NextGen, Dual
- Hosted at [client].traverge.com
- FedRAMP-compatible built on ZTA
- Agency access without approval gates
- Programmatic API delivery for all artifacts
- Versioned snapshots for all OCR cycles.

Automated Package Authoring with Paramify GRC.

- **Certification Package Overview (Replaces the SSP)**

  Replaces traditional SSPs with CR26-compliant Certification Package Overviews (CPOs), generated directly from platform metadata with automated schema validation.

- **Comprehensive Security Decision Record Coverage**

  Maintains the 7 items per CR26 rule for Rev5 security controls and the 20x KSIs (plus daily metrics), exporting in human-readable and machine-readable formats.

- **Automated Maintenance Cadence**

  Executes package updates every two weeks for 20x programs and yearly for Rev5, continuously validating outputs against the FedRAMP schemas.

- **Automated Quarterly Reporting**

  Aggregates data directly from source systems to generate all 8 required OCR cycle summaries automatically without manual assembly.

- **Live Marketplace Data Sync**

  Maintains your FedRAMP Marketplace listing as an active dataset, automatically synchronizing Certification Data in dual formats during every OCR cycle.

PARAMIFY GRC AT A GLANCE

- Applies to Legacy, NextGen, Dual, Custom
- Supports legacy SSP or CPO and SDR
- 11 FedRAMP schema validations
- Rev5: ConMon Support
- 20x bi-weekly maintenance
- Auto-populates OCR report summaries.

Hands-Off ConMon Execution for Rev5 Authorizations.

- **Monthly Scan Ingestion & Root-Cause Triage**
  Direct ingestion and root-cause classification for all scanner findings, separating vendor issues, false positives, operational requirements, and validated fixes while starting SLA timers instantly.
- **Enforced POA&M Lifecycle Management**
  Full oversight of open findings against strict FedRAMP SLA windows. Automated escalation triggers before deadlines breach to ensure complete tracking through final disposition.
- **CR26 Security Decision Record (SDR) Management**
  False positives and operational exceptions are drafted, packaged, and submitted as official SDRs to the PMO, executing the required CR26 replacement for legacy deviation requests.
- **On-Time Monthly ConMon Package Delivery**
  Complete monthly assembly and submission of all required PMO and agency reporting deliverables, including executive status dashboards and technical reporting assets.
- **Continuous Certification Readiness**
  Continuous logging of operational evidence and active upkeep of package documentation ensure your program stays fully defensible between formal assessment cycles.

WHAT THIS MEANS FOR REV5 HOLDERS

- Zero internal ConMon overhead
- SLA tracking prevents breaches
- SDR submissions replace legacy DRs
- POA&M management and enforcement
- PMO deliverables always on time
- Audit trail maintained continuously

Fully Managed 20x Continuous Certification Operations

- **KSI Continuous Validation**

  Automated, real-time evidence collection against all applicable Key Security Indicators. Machine-readable output delivered continuously to the FedRAMP PMO.

- **Ongoing Certification Report (OCR) Lifecycle**

  Quarterly OCRs produced and delivered to all required parties, covering certification data changes, accepted vulnerabilities, planned changes, and incident summaries.

- **Security Decision Record (SDR) Management**

  Accepted vulnerabilities, risk decisions, and control deviations are documented and maintained as Security Decision Records. Continuously updated as your environment evolves.

- **Vulnerability Detection and Response (VDR)**

  Continuous automated detection across CVE scanning, configuration drift, and SDR accuracy. Not limited to traditional vulnerability types. ITSM tickets assigned to your operations team with SLA enforcement against PAIN N-ratings per CISA BOD 26-04.

- **Vulnerability Evaluation and Reporting (VER)**

  Each finding scored for exploitability (LEV), internet-reachability (IRV), and Potential Agency Impact N-rating (PAIN N1-N5). Monthly machine-readable reports delivered to the FedRAMP PMO and your agency customers.

KEY 20X DIFFERENCES

- No POA&M required
- No monthly ConMon packages
- OCRs replace monthly reporting
- KSI validation is continuous
- SDRs document all risk decisions (No DRs)
- VDR and VER fully managed end-to-end

ITSM built for FedRAMP-regulated environments

For many customers, the FRaaS ITSM replaces tools like Jira, removing compliance gaps from managing FedRAMP obligations through a platform not designed for them.

Security Incident Management

- Incident escalation aligned with federal reporting rules
- Rapid triage, containment, and root-cause analysis
- Direct ticket routing to designated on-call security leads
- Immutable ticket history saved as permanent audit evidence

Configuration Management and Change Control

- Screening for system boundary, data type, and PPS changes
- System Privacy Impact Assessment (SPIA) Evaluations
- SCN categorization by FedRAMP SMEs satisfying CR26
- Risk reviews linked directly to approval and deployment logs

Identity and Access Management

- User access requests (onboarding, modifications, and offboarding)
- SLA enforcement for expeditious revocations and terminations
- Repository for background checks, NDAs, signed RoBs, etc.
- Enforced quarterly reviews to ensure least-privilege compliance

Vulnerability and POA&M Lifecycle

- Automatic ITSM ticket generation for confirmed vulnerabilities
- Automated alerts prior to SLA compliance deadline breaches
- Tracking from initial scanner detection through final disposition
- Integrated packaging for SDRs and accepted risk exceptions

SHARED RESPONSIBILITY MODEL

A clear line between what we own and what you retain

The boundary is defined in your contract from day one and does not change. Traverge carries the operational weight so your team stays focused on what only you can do.

TRAVERGE MANAGES

- Fully Managed ConMon (Rev 5 and 20x): day-to-day operations, monthly packages, scan ingestion, POA&M
- ITSM Ticketing: end-to-end lifecycle for vulnerabilities, changes, access, and incidents
- Continuous GRC and Machine-Readable: real-time SSP updates and documentation automation via Paramify
- Independent Assessor Support: full facilitation, evidence delivery, and audit defense
- Continuous Certification Readiness: program posture maintained between assessment cycles

YOU RETAIN

- Core application engineering, product development, and feature delivery
- Independent assessor selection (choose from Traverge's partner network or bring your own)
- SME representation during auditor interviews
- Vendor contracts and third-party tool and infrastructure agreements

FRAAS PACKAGES

Pick your path

Three fixed-fee packages cover every FedRAMP posture. If none of them fit exactly, FRaaS Custom is structured around your program.

LEGACY

FRaaS Legacy

Rev5 ATO holders

Maintain your existing Rev5 certification through CR26 mandates, including the FedRAMP JSON/OSCAL migration.

- Monthly ConMon operations
- POA&M lifecycle management
- JSON/OSCAL package maintenance
- ITSM, vuln tracker, SCN manager
- Paramify GRC platform included

FedRAMP Mod (Class C)

NEXTGEN

FRaaS NextGen

New 20x programs

For CSPs entering the FedRAMP Marketplace directly via 20x, from initial certification through ConMon.

- FedRAMP 20x certification support
- KSI evidence collection and validation
- Real-time JSON/OSCAL generation
- ITSM, vuln tracker, SCN manager
- Paramify GRC platform included

FedRAMP Mod (Class C)

DUAL

FRaaS Dual

Multi-market providers

Maintain active Rev5 and 20x certifications at the same time during transition or for multiple markets.

- Dual-framework ConMon management
- JSON/OSCAL remediation in scope
- 20x KSI validation alongside Rev5
- ITSM, vuln tracker, SCN manager
- Paramify GRC platform included

FedRAMP Mod (Class C)

CUSTOM

FRaaS Custom

Unique requirements

If Legacy, NextGen, or Dual don't quite fit, Traverge structures a service around your program.

- Scoped to your program
- Fixed-fee or T&M available
- Any FedRAMP framework combination
- ITSM, vuln tracker, SCN manager
- Paramify GRC platform available

FedRAMP Mod (Class C)

THE TEAM

Practitioners, not generalists

Every FRaaS engagement is led by someone who has spent over a decade doing exactly this, at the highest levels of the federal government. Not compliance-adjacent. Not cross-trained from another practice.

40+

Combined years of FedRAMP operational experience across the delivery team

12+

Years of dedicated federal cloud cybersecurity experience, minimum, per practitioner

60+

Initial and annual FedRAMP certification assessments lead

DIRECT OPERATIONAL EXPERIENCE (partial)

- USSOCOM
- Defense Health Agency
- State Department
- White House
- Veterans Affairs
- Homeland Security
- Air Force Global Strike Command
- United States Space Force
- Health and Human Services
- FBI
- IL-4 / IL-5 / IL-6

> *"Too many major FedRAMP firms lure clients in with their top talent during sales pitches, only to bait-and-switch them with mid- or junior-level advisors once the contract is signed. The experts in our sales meetings are the exact same practitioners on your program."*
>
> Jonathan Riddle, Founder and CEO, Traverge

NEXT STEPS

1. Tell us where your program is today
2. We identify the right FRaaS package
3. Proposal with defined scope and fixed fee
4. Onboarding in 30 days or less

TRAVERGE
UNIFIED COMPLIANCE - SIMPLIFIED SECURITY™

FRaaS
FedRAMP-as-a-Service

Ready to get off the compliance rollercoaster?

Tell us where your program is today. We will tell you which FRaaS package fits and what onboarding looks like.

Talk to a FedRAMP practitioner

contact@traverge.com

traverge.com

(904) 257-6192

12724 Gran Bay Parkway West, Suite 410 | Jacksonville, FL 32258

The experts you meet in this conversation are the practitioners leading your program.

SBA
U.S. Small Business Administration
SERVICE-DISABLED VETERAN-OWNED CERTIFIED