cuick trac™
BY BERYLLIUM INFOSEC

# The Simple Path to Compliance

**A deeper look at how the Cuick Trac Managed Enclave accelerates secure CUI workflows and CMMC Level 2 alignment**

# Table of Contents

# Introduction



Cuick Trac was founded in 2018 by Beryllium InfoSec, a Dallas-based cybersecurity and compliance firm founded to serve the Defense Industrial Base (DIB). With over 100 years of combined experience, our team specializes in helping government contractors protect Controlled Unclassified Information (CUI) and meet evolving federal cybersecurity requirements.

Built by the same experts who manage it today, the Cuick Trac Managed Enclave (CTME) is a purpose-built solution that simplifies compliance with **DFARS 252.204-7012, NIST 800-171, and CMMC Level 2.** It provides contractors with a faster, more practical way to secure CUI, without the need to overhaul their entire IT environment.

In the fall of 2024, Beryllium InfoSec—operating as a Cloud Service Provider (CSP)—and its core product, the Cuick Trac Managed Enclave (CTME), a Cloud Service Offering (CSO), achieved FedRAMP Moderate Equivalency through an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization (3PAO). In early 2025, Beryllium InfoSec successfully completed a CMMC Level 2 Certification for its internal system, powered by CTME, through a third-party assessment by an authorized C3PAO. These milestones confirm that CTME meets the Department of Defense's rigorous standards for protecting Controlled Unclassified Information (CUI) and supports other organizations seeking to do the same.

> **This guide is for contractors and partners ready to understand how the Cuick Trac Managed Enclave actually works—from provisioning and inherited controls to real-world results.**

### Industry Related Certifications & Subject Matter Expertise:

NIST SP 800-53
NIST SP 800-171 & 172
NIST SP 800-161 - Supply Chain Risk Management
NIST SP 800-160 volume 1 - Systems Security Engineering
ISC2 Certified in Governance Risk & Compliance (CGRC)
Federal Risk and Authorization Management Program (FedRAMP)
Federal Information Security Management Act (FISMA)
Federal Acquisition Regulation (FAR)
Defense Federal Acquisition Regulation Supplement (DFARS)
Risk Management Framework (RMF)
(ISC)2 Certified Information Systems Security Professionals (CISSP)
DoD Information Assurance Systems Architects & Engineers (IASAE)
Information Technology Infrastructure Library (ITIL) v3
Greenbelt Lean Six Sigma
CompTIA Network +
CompTIA Security +
CompTIA A +

### Credentials recognized by the CyberAB:

Registered Provider Organization (RPO)
CMMC Lead Assessors (Lead CCA)
CMMC Certified Assessors (CCA)
CMMC Certified Professionals (CCP)
CMMC Provisional Instructor (PI)
Registered Practitioners (RP)

# Compliance Challenges in the DIB

Cybersecurity compliance in the Defense Industrial Base (DIB) has become a moving target. Defense contractors are required to meet an evolving set of technical and procedural standards—most notably DFARS 252.204-7012 and NIST SP 800-171—as a condition of doing business with the U.S. Department of Defense. With the rollout of the Cybersecurity Maturity Model Certification (CMMC), these requirements have become stricter, more formalized, and increasingly enforceable.

Unfortunately, the burden of compliance typically falls on small to midsize businesses (SMBs) who lack the time, internal expertise, or budget to build and manage a secure, compliant IT environment. **This creates a web of operational, financial, and security challenges that most tools fail to address holistically.**

- **Cost & Expertise**
  High costs and limited access to in-house experts
- **Incomplete Solutions**
  Many tools only address pieces of the full compliance picture
- **Usability**
  Most solutions are hard to implement, manage, or understand
- **Controlled Unclassified Information (CUI) Security**
  Few offerings effectively isolate CUI from broader networks
- **Operational Inefficiency**
  Slow processes, manual documentation, and audit fatigue

While some competitors focus on a single aspect—like documentation or cloud storage—The Cuick Trac Managed Enclave solves the full equation: technology + security + compliance. Our comprehensive platform addresses the root challenges while eliminating the need for multiple vendors, costly rebuilds, or heavy in-house oversight.

> **This all-in-one approach gives contractors the clarity, speed, and confidence they need to protect CUI and maintain contract eligibility.**


# Our Solution

The Cuick Trac Managed Enclave (CTME) is a fully managed security enclave and turnkey compliance solution with FedRAMP Moderate Equivalent status. CTME simplifies compliance with DFARS 252.204-7012, NIST SP 800-171 and CMMC Level 2. It's a secure, compliant, and scalable environment designed for handling Controlled Unclassified Information (CUI) without requiring you to re-architect your internal IT or rip and replace your existing infrastructure.

**More than just a product, the Cuick Trac Managed Enclave is a complete system engineered for real-world outcomes:**

### Cost Effective

Save thousands, potentially more, on implementation and management with all-in, transparent costs, without increasing staff.

### Expert-Driven

Our team includes in-house CMMC Compliance Managers who deliver trusted, expert guidance.

### Simple & Seamless

Pre-built, rapidly deployable, and designed to integrate with your current workflow.

### Fast Deployment

Once your domain is selected and we've received your CUI access list, users can be ready for onboarding in 15 days.

### Scalable & Flexible

Works for 10-person teams or 500-supplier networks, with no major infrastructure changes required.

### Dedicated Help Desk

Our expert support team is here to assist Cuick Trac users with technical support and assistance, ensuring smooth operations.

## The Compliance Support Space

| 90% GRC Tools, RPOs, MSPs, vCISOs | | | 10% Real Solutions | |
|---|---|---|---|---|
| **Needs** → | **Current State Analysis** → | **Plan Development** → | Cuick Trac **Solves the Problem** → | **Assess + Certify** |
| "We need to protect CUI and meet compliance requirements." | "What do we have in place?" | "Here's what we need to do." | Implement a secure, managed environment that meets the technical requirements. | Third-party C3PAO comes in to verify compliance. |

# How it Works

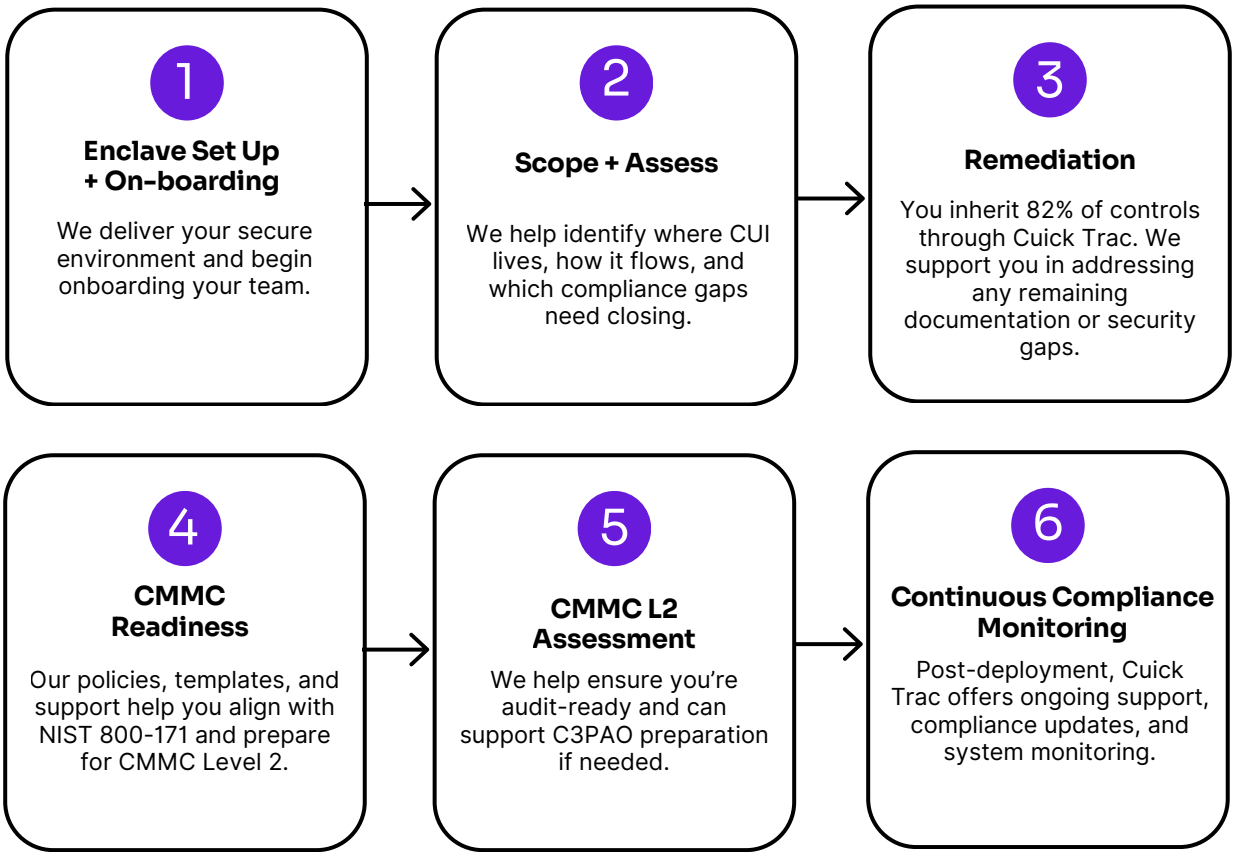
The Cuick Trac Managed Enclave is designed to make onboarding and compliance simple—without sacrificing security, control, or audit-readiness. Our process is both fast and thorough, guided by experienced advisors and built for minimal disruption

## Implementation Timeline

Once your domain is selected and we've received your CUI access list...

Users will be ready for onboarding in as few as **15 business days**

## Customer Journey

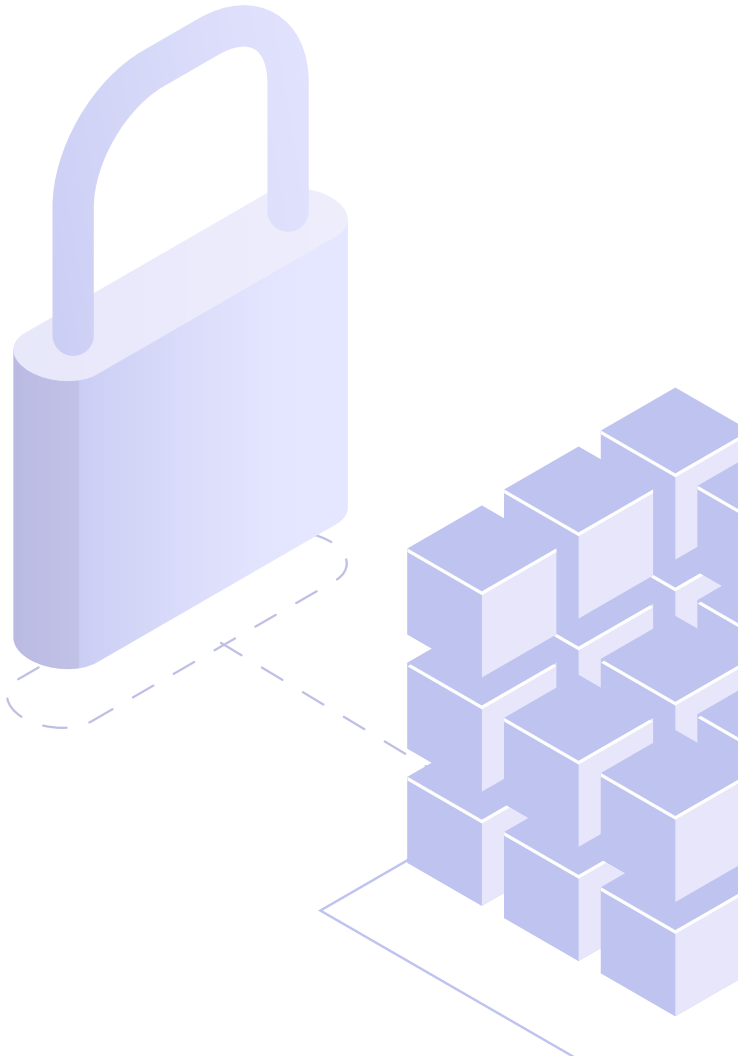


# What's Included

The Cuick Trac Managed Enclave delivers **more than just secure hosting**. It's a purpose-built compliance ecosystem that combines the tools, protections, and guidance you need to protect Controlled Unclassified Information (CUI) and meet federal security mandates with confidence.

**Here's what you actually get:**

- → Virtual Desktop Infrastructure
- → FedRAMP Moderate Equivalent Enclave
- → Used to pass CMMC Level 2 Certification Assessments by C3PAOs
- → Controlled digital CUI data flows - device out of scope
- → Full System Administration
- → Managed SIEM
- → Encrypted Storage
- → Encrypted Email
- → MFA
- → SharePoint
- → Microsoft GovTeams
- → Zero Trust Principles
- → Incident Response Plan
- → System Security Plan (SSP)
- → Backup and Retention
- → Penetration Tested
- → Third-Party Red Team Tested
- → Secure File Sharing for larger files
- → Help Desk + Support
- → CUI Data Flow Diagram
- → Policies, Standards, and Procedures



# Customer Success Stories

## How We Helped a Top Defense Prime Strengthen Their Supply Chain

**The Challenge:**

- Limited visibility into lower-tier suppliers
- Risk of non-compliance from resource-constrained SMBs
- No scalable way to ensure cybersecurity readiness across the supply base

**The Solution:**

- Cuick Trac deployed across dozens of suppliers starting in 2019
- Combined the Cuick Trac Managed Enclave (CTME) with expert advisory services from the Cuick Trac team
- Suppliers onboarded in as few as 10 business days

**The Result:**

**Suppliers using Cuick Trac achieved higher compliance scores and greater audit readiness. The prime gained confidence in its supplier base without needing to increase oversight—reducing risk and improving supply chain visibility.**

## How a Managed Service Provider (MSP) Retained Their Client and Grew Their Business with Cuick Trac

**The Challenge:**

- MSP client—a small government contractor—faced rising DFARS and CMMC compliance requirements
- MSP lacked internal expertise in federal cybersecurity compliance
- Risk of losing a long-time client due to inability to support evolving needs

**The Solution:**

- MSP partnered with Cuick Trac to deliver a turnkey compliance solution
- Deployed an audit-ready CUI enclave while preserving the MSP's role in managing broader IT infrastructure by removing their CUI scope
- Enabled compliance support without requiring the MSP to rebuild its service model

**The Result:**

**After a successful implementation, the MSP retained the client and began offering the Cuick Trac Managed Enclave (CTME) to other businesses in the region, turning compliance challenges into a competitive advantage.**

# FAQs

## Does Cuick Trac replace my MSP provider or internal IT team?

No. With Cuick Trac, our goal is to always work with as much of your current business processes that are already in place, including your current MSP or internal IT team. Disruption to your business is detrimental; thus, a collaborative approach will be key in regard to how CUI data is collected, stored and accessed.

As a FedRAMP Moderate Equivalent Cloud Service Offering (CSO) from a Cloud Service Provider (CSP), your MSP or internal IT team can leverage Cuick Trac for your CUI program, lowering the burden internally.

## Do I need a System Security Plan (SSP) and Plan of Actions and Milestones (POA&M) Before Utilizing Cuick Trac?

No. If an organization knows it isn't compliant, it needs to focus on solutions that best fit its business. A Cuick Trac subject matter expert (SME) will help an organization identify CUI data flow, scope, and boundary. Once the identified users in scope are using the Cuick Trac enclave, the customer and Cuick Trac conduct an assessment of the NIST SP 800-171A assessment objectives using the CMMC Assessment and Scoping Guides and create/update the SSP. All remaining gaps become the POA&M (physical and administrative controls outside of the Cuick Trac enclave, if applicable) and shorten the path to completing your plan of full implementation and ongoing/continuous compliance.

## What happens if I'm not compliant with DFARS/NIST 800-171?

Besides the risk of failing a future CMMC certification, organizations that fail to prove that they have NIST SP 800-171 fully implemented and continuously monitored will lose the opportunity to be awarded new DoD contract awards, and potentially face fines or loss of contract.

## We don't have a SIEM or any way to monitor incidents, events, or breaches. Does Cuick Trac do that?

Yes. Under the DFARS clause, contractors must report cyber incidents within 72 hours of them happening. That's a difficult thing to accomplish if your business doesn't have the personnel or resources to always be monitoring your security information and event management solution (SIEM). Cuick Trac has a SIEM monitoring the enclave, and that information is reviewed by Cuick Trac security analysts and reviewed with Cuick Trac customers on a regular basis.

# Next Steps

Whether you're trying to win your first DoD contract or need to ensure hundreds of suppliers meet compliance requirements, Cuick Trac can help you move forward quickly and confidently.

## Here's what to do next:

### Book a 30-Minute Discovery Call

Meet with a Cuick Trac product expert to assess your current compliance posture and determine whether our platform is the right fit. No pressure, just insight.

→ **Explore Deployment Options:** We'll show you exactly how Cuick Trac can be deployed in your environment (or across your supplier base), how long it will take, and what you'll need to get started.

→ **Understand Pricing and ROI:** Our team will walk through transparent pricing models and expected time/cost savings, based on your business size, compliance stage, and risk profile.

**Get in touch on our website: www.cuicktrac.com/contact/**

**612-428-3008**

**www.cuicktrac.com**