Cloud-Based CUI Enclaves

A CMMC Compliant Approach

Organizations Seeking Certification (OSC)

The path to CMMC Level 2, from preparation to certification and beyond.

STEP 1 · PREPARE

1. **Identify Level 2**
2. **Engage a CMMC Pro**
3. **Identify Scope**
4. **Conduct Gap Assessment**
5. **Complete All Projects**
6. **Perform Assessment**

STEP 2 · CHOOSE YOUR CERTIFICATION PATH

C3PAO Assessment

3-YEAR

- → Identify C3PAO
- → Schedule assessment
- → Pass Level 2 assessment
- → Receive CMMC-AB certificate

Level 2 Self-Attestation

1-YEAR

- → Complete self-assessment
- → Post results to SPRS
- → Sign-off by authorized official

Then maintain: affirm and sustain your CMMC assessment level on an ongoing basis.

Where Does Your CUI Live?

Contain it. The enterprise is your whole business. An enclave (the shed) is a small, deliberate space that holds the CUI, so everything else stays out of scope.

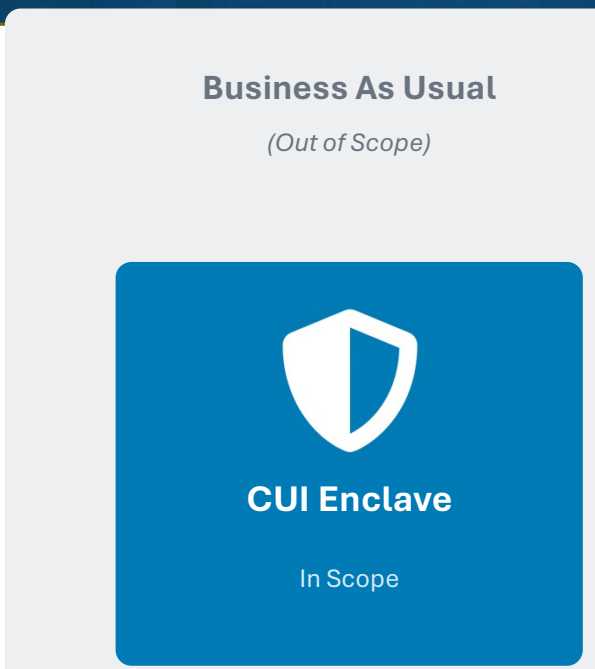
Or chase it everywhere. Without an enclave, CUI scatters across your systems, and every place it lands is pulled into scope.

What is a CUI Enclave?

An isolated and clearly defined boundary for performing specific CUI tasks by a subset of users.

A logically and physically separated environment for processing, storing, and transmitting CUI.

An architectural approach to IT infrastructure that prioritizes segmentation and scope-reduction techniques.



CMMC Scope: Enterprise vs Enclave

Full Enterprise Approach

- Single environment
- Every system and device in scope; full boundary
- Every user is in scope
- CMMC applies to the full enterprise

Enclave Approach

- Separate CUI environment
- Smaller isolated boundary is in scope
- Fewer assets; fewer users in scope
- CMMC applies to the enclave

Key Takeaway: CMMC follows the CUI. Wherever the CUI goes, scope follows. An enclave succeeds by keeping both the CUI and the scope contained within a well-defined, consolidated boundary.

Why Choose A Cloud Enclave?

Better question: **“What problems can a Cloud Enclave solve?”**

- Protect CUI using reduced scope
- Consolidate the assessment boundary
- Avoid rebuilding the enterprise
- Avoid changing existing processes
- Avoid changing IT resources (MSP/Internal IT Staff)
- Provide simple workflows for users
- Accelerate CMMC compliance
- Conserve resources (money, labor, effort)

Cloud Enclave: Advantages

Reduced Scope & Assessment Boundary

Smaller CUI footprint; fully remote assessment

Isolation of CUI from Corporate Systems

Keep the enterprise "as-is" and out-of-scope

Accelerated Deployment & Simplified Security

Faster, cheaper, leaner deployment

Lower Compliance & Operational Overhead

Less admin burden; fewer impacted workflows

Consolidated Visibility, Monitoring & Auditing

Less infrastructure; easier continuous monitoring

Scalable & Repeatable Architecture

Add assets and scale with a single click

CSP Shared Responsibility & FedRAMP

CSP OSC

Compliance is Shared

The CSP secures the foundation.
The OSC still owns protecting the CUI.

- Cloud providers deliver a pre-secured foundation.
- FedRAMP authorization provides independently assessed security controls.
- Organizations can inherit certain controls from the CSP.
- Configuration, identity, data protection, and monitoring must still be managed.
- **Compliance is shared, not transferred.**
- **Responsibility for protecting CUI remains with the OSC.**

Cloud Enclave: Limitations

What are the trade-offs?

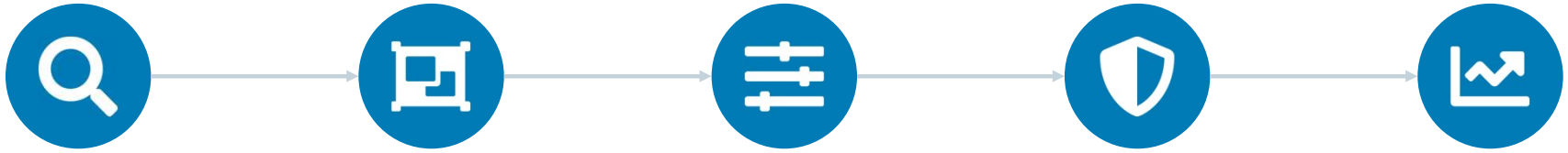
- Limited features / limited functionality
- Added system, management, and process
- Added licensing and cloud-compute costs
- Legacy integrations may not be possible
- No physical CUI

Weigh the Trade-offs

An enclave shrinks scope, but it adds cost and constraints. Know the trade-offs before you commit, and design around what your work truly requires.

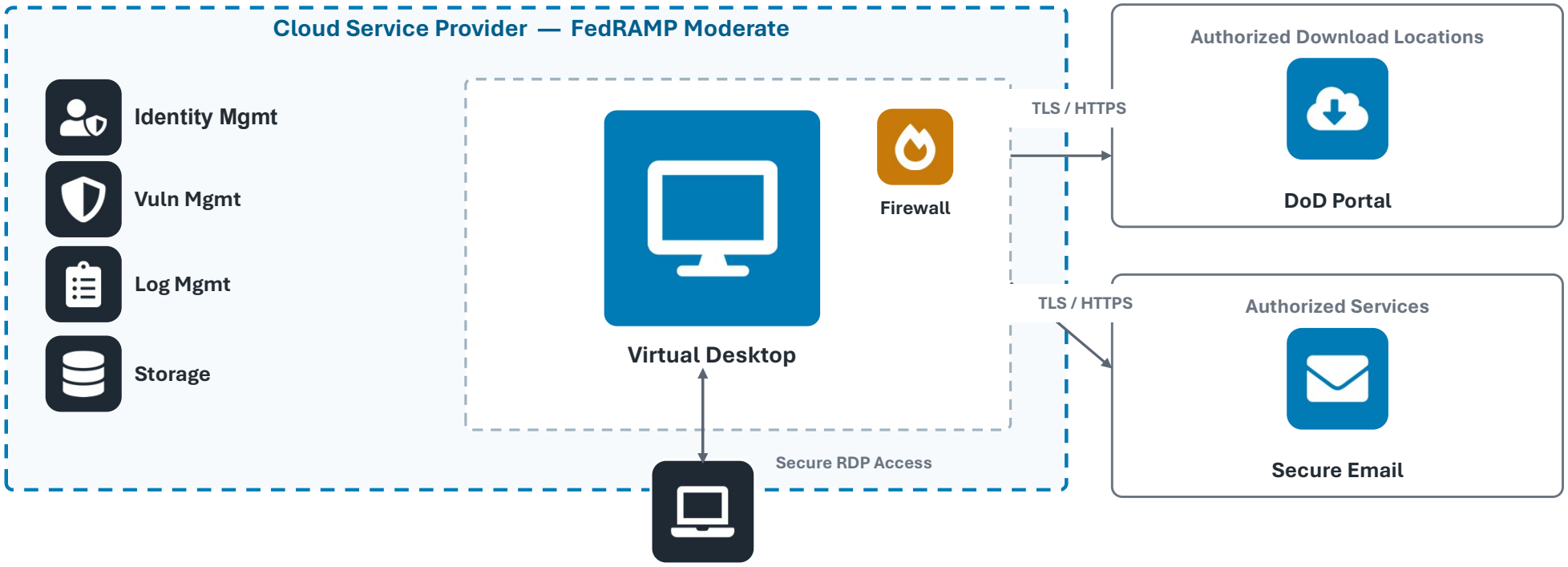
The 5-Step Approach

Thinking about a cloud enclave to meet your CMMC requirement? Start with these five steps.



1. **Identify:** What is CUI; how it enters the enclave; what we do with it; who it is shared with.
2. **Define:** What is in scope: systems, locations, and personnel.
3. **Control:** How access is controlled; how the CUI area is segmented; how storage and processing are controlled.
4. **Secure:** How CUI is protected and how security is implemented.
5. **Monitor:** What evidence we collect; how continuous monitoring runs; how changes and compliance are documented.

CUI Cloud Enclave Example



Key Takeaways

1. **Scope drives everything.** Cost, timeline, and risk all scale with how much of your business touches sensitive data. An enclave shrinks that footprint on purpose.

2. **An enclave is a strategy, not a product.** It is a small, enforced boundary that contains CUI so the rest of your company can stay simple and out of scope.

3. **Cloud usually wins for smaller contractors.** You inherit proven controls and avoid the full build-and-maintain burden.

4. **Platform choice follows your data and ecosystem.** Microsoft, Google, or AWS. FedRAMP authorization is necessary but not sufficient; configuration and documentation still fall to you.

Bottom line: For most contractors, an enclave is the most reliable way to turn an overwhelming, open-ended compliance problem into a small, predictable, affordable one. Understand the boundary, respect what it cannot do, choose the version that fits your data and team, and you can have that conversation as a peer.

Questions?

Thank you. Let’s talk about right-sizing your CUI enclave.

Rob Panek

Security Cavalry

360.930.6989

Rob@SecurityCavalry.com

SecurityCavalry.com