EXOSTAR / CMMC READY SUITE™

EXOSTAR

Defense runs on CUI. **Protection starts in the enclave.**

Managed enclave | CUI friendly | GCC High | Secure virtual desktop

Protect CUI. Keep sensitive conversations secure.

Exostar's CMMC Ready Suite brings protection and proof together in a managed environment. Give authorized people a controlled place to store, share, and work with sensitive information—and keep downloaded files in a secure environment.

Build your documentation and evidence to demonstrate how you protect CUI, so your team can keep defense work moving.

A MANAGED ENCLAVE ENABLES:

- Store CUI securely
- Process CUI inside a managed virtual desktop
- Collaborate with approved partners
- Reduce local downloads and endpoint exposure
- Maintain a clear CMMC scope boundary

THE JOURNEY OF CUI INSIDE THE ENCLAVE

1. Generate CUI
2. Share CUI to the enclave
3. Sign in via virtual desktop
4. Access CUI based on roles
5. Complete work inside the enclave

CUI stays protected from start to finish.
All storage, processing, and sharing happens inside the managed enclave.

Benefits of a managed enclave

SIX WAYS THE ENCLAVE WORKS FOR YOU

- Controlled file sharing
- No local downloads
- Managed CUI workspace
- Controlled CUI storage
- Authorized access
- Support audit visibility

Protect CUI. **Demonstrate control.**

Every activity builds on one foundation: a controlled environment where CUI is securely stored, processed, and transmitted.

THE MANAGED ENCLAVE

Everything happens inside the managed enclave. CUI stays protected through its lifecycle while organizations maintain a smaller, easier-to-manage CMMC scope.

1 **Log in**

2 **Launch the virtual desktop**

3 **Work and collaborate securely**

STORE
Secure storage in Microsoft 365 GCC High

PROCESS
Work with CUI inside the enclave

SHARE & TRANSMIT
Work with authorized recipients and securely share CUI approved users and partners

Protect CUI and prove it

Keep documentation and evidence current to show how CUI is protected.

01
Define the scope
Map CUI workflows and determine assessment boundaries.

02
Compliance documentation
Generate SSPs, POA&Ms, policies, and calculate SPRS scores.

03
Collect evidence
Capture artifacts continuously throughout implementation.

04
Close gaps
Prioritize remediation and track progress.

05
Demonstrate protection
Keep documentation and evidence current to show how you protect CUI.

TALK TO SALES

Ready to protect the CUI your defense work depends on?

Talk with Exostar about protecting your CUI workflows.

Talk to Sales →

exostar.com

© 2026 Exostar. All Rights Reserved.