

CMMC READY SUITE™ | SOLUTION BRIEF

A tangible, defensible path to protecting Controlled Unclassified Information

Exostar's CMMC Ready Suite™ helps organizations build a secure foundation for protecting CUI while simplifying documentation, evidence management, policy creation, and ongoing compliance activities.

Secure CUI Collaboration

Compliance Automation

Professional Services

Organizations that handle Controlled Unclassified Information (CUI) are contractually required to protect it under DFARS 252.204-7012 by implementing the applicable NIST SP 800-171 Revision 2 security requirements. While the Department of War has suspended the planned expansion of CMMC third-party assessments, organizations must still secure where CUI is stored, processed, and transmitted, complete required self-assessments where applicable, maintain documentation, and submit affirmations through SPRS.

CMMC readiness requires more than software

For organizations that support the Department of Defense, CMMC readiness is not simply a checkbox exercise. It affects how teams collaborate, where sensitive information is stored, how users access systems, how evidence is collected, and how security practices are documented.



Collaboration on CUI

Email, unmanaged devices, and commercial collaboration tools make it hard to control where CUI goes or prove how it is protected.



Documentation burden

Manual SSPs, POA&Ms, policies, score reports, and evidence are time-consuming and hard to keep up to date.



Expertise gaps

Internal teams may lack the compliance expertise or bandwidth to manage the full readiness process alone.



Self-assessment readiness

Technology alone does not close every control gap, organize every artifact, or prepare teams for assessment conversations.



Legacy systems

Older dependent platforms and manual processes are difficult to secure, hard to document, and not built for modern controls.



Specialized equipment

Operational technology and purpose-built systems cannot be easily modified without affecting production or mission requirements.



Budget and resource constraints

Security improvements must balance risk reduction with implementation complexity, operational impact, and the realities of day-to-day business.

Technology + services for CMMC readiness

The result of those challenges is often confusion, delay, competing priorities, and unpredictable cost. Exostar's CMMC Ready Suite™ is built to address that reality: CMMC readiness takes both technology and services, along with a practical approach to reducing risk without creating unnecessary complexity.

Exostar's CMMC Ready Suite™ provides a practical path to CMMC Level 2 readiness, bringing together the core capabilities needed to secure CUI, manage compliance activities, create defensible documentation and objective evidence, and prepare for the assessment process — aligned to the customer's CUI use case, readiness maturity, and assessment path.

01 Identity and access management

Strong authentication, role-based access, and secure collaboration with internal and external users.

02 Secure CUI collaboration

Store, share, and collaborate on sensitive information in a managed environment.

03 Compliance management automation

Guide self-assessments, calculate SPRS scores, generate SSPs and POA&Ms, track progress.

04 Automated policy generation

Create policies that reflect how the organization actually operates, not generic templates.

05 Professional readiness services

Scoped to the customer's readiness needs — identify gaps, prioritize remediation, organize evidence, and prepare for the applicable self-assessment.

Technology components



Managed Access Gateway

Identity & access

Only authorized, verified users reach CUI environments — authentication, MFA, and company/user proofing.



Exostar's Managed on Microsoft 365™

Secure CUI enclave

A managed, auditable enclave for CUI that keeps endpoints and enterprise systems out of scope.



Managed Secure Desktop™

Controlled workspace

A virtual desktop for CUI work that limits downloads and sharpens the scope boundary.



Secure Exchange™

Controlled exchange

Approved inbound and outbound workflows replace email and unmanaged file-sharing for CUI.



Certification Assistant™

Compliance management

Self-assessment, SPRS scoring, SSP and POA&M generation, and evidence organization in one place.



PolicyPro™

Policy automation

Assessment-ready policies generated from how your organization actually operates.

Managed Access Gateway (MAG)

Exostar's Managed Access Gateway provides the identity and access foundation for CMMC Ready Suite™. It serves as the secure front door for users accessing Exostar's CMMC-related applications and managed collaboration environments, helping ensure that only authorized users with appropriate credentials can enter the systems where readiness work and secure collaboration occur.



User onboarding

Streamlined account creation and enrollment



Authentication & MFA

One-time password credentials, PKI certificates, third-party credentials such as CAC/PIV, and company credentials through Enterprise Access Gateway



Access workflows

Centralized gateway for application access, terms and conditions, and single sign-on



Company proofing

Verification of organizational identity and affiliation

MAG helps control access across CUI collaboration and compliance readiness environments by combining secure authentication, MFA, company and user proofing, and application-level access workflows. This reduces access complexity, strengthens governance, and supports a controlled path to CMMC Level 2 readiness.

Exostar's Managed on Microsoft 365™

At the center of CMMC Ready Suite™ is Exostar's Managed on Microsoft 365™, a managed, auditable enclave designed for organizations that need to store, monitor, share, and secure CUI and ITAR/export-controlled documentation without turning their entire corporate network into the compliance boundary.

Key capabilities

- Microsoft 365 GCC High enclave
- SharePoint secure storage
- Role-based access control
- Compliant File Drop
- 24/7 SOC monitoring
- Microsoft Teams collaboration
- Managed Access Gateway authentication
- Domain allowlisting
- Centralized reporting and audit logs
- Download restrictions

Available applications

Microsoft Teams

SharePoint Online

Microsoft Lists

Planner

Word

Excel

PowerPoint

Visio

OneNote

Office web applications, offered as a limited, security-controlled set.

The service combines Managed Access Gateway, Microsoft 365 GCC High, and Security Operations Center monitoring to support secure collaboration in a controlled environment. Users work in familiar Microsoft tools while Exostar provides the identity, governance, monitoring, and managed service capabilities needed for CMMC readiness — reducing IT burden, limiting scope, and making partner collaboration more controlled.

Managed Secure Desktop™

Managed Secure Desktop™ extends Exostar's Managed on Microsoft 365™ by giving users a controlled workspace for accessing and working with CUI inside the managed enclave. This helps solve a critical challenge: teams need to work with sensitive information, but organizations don't want CUI spreading across local laptops, email inboxes, or unmanaged systems.

- Reduced risk of CUI downloads on unmanaged devices
- Clearer separation between CUI workflows and corporate systems
- Support for users who actively work with CUI
- Partner collaboration without distributing uncontrolled copies

What stays inside the enclave



The workspace

Users open a managed virtual desktop instead of working on a local machine.



The files

CUI is opened, edited, and stored inside the enclave — no local copies.



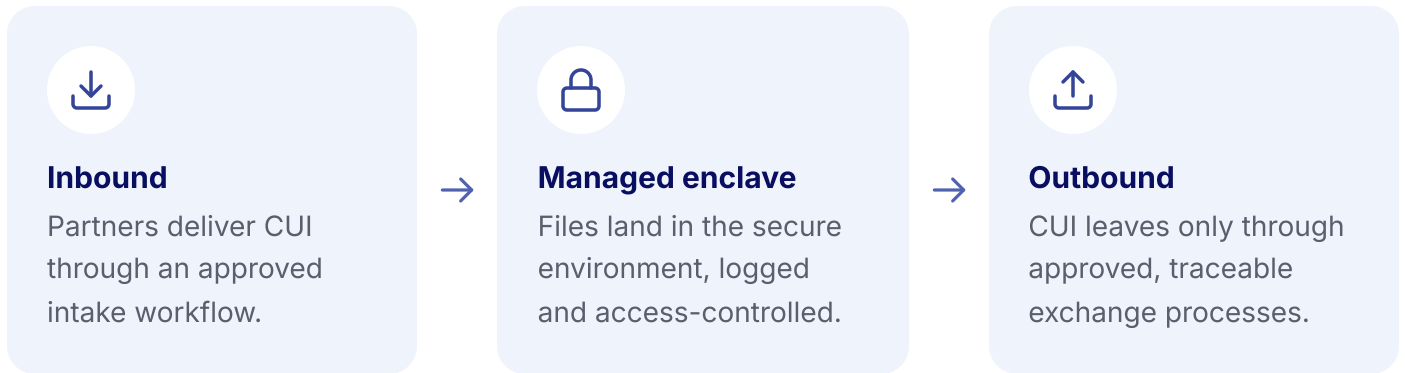
The boundary

Endpoints stay out of scope, so the assessment boundary is clearer.

Secure Exchange™

Secure Exchange™ helps organizations move CUI through more controlled workflows inside the managed environment. Instead of relying on standard email attachments or unmanaged file-sharing methods, teams use approved inbound and outbound exchange processes that keep sensitive information connected to the secure collaboration environment.

How CUI moves



CUI can still move when business requires it, but with more structure, control, and visibility. This reduces reliance on email-based workflows, supports partner collaboration, and creates a more consistent process for CUI exchange as part of broader CMMC readiness efforts.

Certification Assistant™

Once CUI collaboration is controlled, organizations still need a way to assess, document, and track readiness. Certification Assistant™ provides a centralized compliance management platform that guides organizations through NIST SP 800-171 and CMMC self-assessment activities.

- Guided self-assessment workflows
- Automated SPRS score calculation
- SSP generation from inputs
- POA&M creation and tracking
- Evidence upload and organization
- Role-based access control
- Task assignment and accountability
- MSP and expert collaboration

WITHOUT

- Scattered spreadsheets and manual scoring
- Evidence spread across inboxes and drives
- SSPs and POA&Ms rebuilt by hand each cycle

WITH CERTIFICATION ASSISTANT™

- Guided workflow with automated SPRS scoring
- Evidence organized against each control
- Living SSP and POA&M, ready for affirmation

Certification Assistant™ helps teams replace scattered spreadsheets and manual scoring with a structured, centralized process. SPRS affirmations and current CMMC status remain important parts of the CMMC program and related DFARS requirements, including annual affirmations of continuous compliance for applicable systems.

PolicyPro™

Policies are among the most difficult aspects of CMMC readiness. Many organizations start with generic templates, but those often fail to reflect how the business actually operates. PolicyPro™ uses guided questionnaires to capture how the organization handles security practices across CMMC domains, then generates policies based on those operational inputs.

How it works

01

Answer

Guided questionnaires capture how your organization actually handles each CMMC domain.

02

Generate

Policies are produced from those operational inputs — not generic templates.

03

Maintain

Update answers as practices change; policies stay consistent and assessment-ready.

The result is policy documentation that is more consistent, easier to maintain, and better aligned to real-world processes. This improves documentation quality, reduces policy-writing effort, and gives teams a stronger foundation for assessment discussions.

Professional services and flexible packages

Technology can accelerate CMMC readiness, but it cannot do everything. Customers still need help interpreting requirements, defining scope, validating documentation, prioritizing gaps, organizing evidence, and preparing for self-affirmation. Exostar's CMMC professional services support the full readiness journey, from current-state review through assessment preparation.

WHAT EXOSTAR DOES

Preparation for CMMC assessment

CMMC experts help customers get ready through gap analysis, remediation support, and documentation preparation.

WHAT YOU GET

A clearer path to readiness

More confidence before assessment, with documentation and evidence organized and gaps prioritized.

Services may include

- CMMC Level 2 readiness review
- Control implementation guidance
- Evidence review and organization
- Shared responsibility guidance
- Gap analysis
- SSP and POA&M support
- Remediation planning
- Policy and documentation review

Exostar readiness and assessment support services help customers prepare for and navigate the assessment process; certification decisions are made through the applicable CMMC assessment process and authorized assessment entities.

How CMMC Ready Suite™ works together

CMMC Ready Suite™ supports the full readiness lifecycle, from access control through assessment preparation and ongoing compliance maintenance.

01

Control user access

MAG and MFA help ensure secure authentication and controlled access for internal and external users.

02

Secure the CUI environment

Managed on Microsoft 365™ provides a managed enclave for CUI. Managed Secure Desktop™ limits CUI activity on unmanaged endpoints.

03

Assess current readiness

Certification Assistant™ guides the organization through self-assessment and readiness tracking.

04

Generate and organize documentation

Generate SSPs, manage POA&Ms, track scores, upload evidence, and organize readiness artifacts.

05

Create assessment-ready policies

PolicyPro™ automates policy creation using real operational inputs across CMMC domains.

06

Identify and close gaps

Consultants work alongside the customer to review results, refine the SSP and POA&M, and identify actions to close control gaps.

07

Prepare for the assessment path

Readiness services organize evidence and align SSP content, policies, and supporting artifacts so they are complete and consistent.

08

Maintain readiness over time

Ongoing compliance management, policy updates, secure collaboration, and documentation maintenance.

Key benefits of CMMC Ready Suite™



Faster path to readiness

Guided workflows, managed technology, automated documentation, and readiness services reduce time to readiness.



Lower total cost of ownership

Bundled technology and services reduce fragmented spending with a predictable pricing model.



Reduced compliance scope

Isolating CUI in a managed enclave reduces the burden of bringing broader systems into scope.



Assessment-ready documentation

Certification Assistant™ and PolicyPro™ generate and maintain SSPs, POA&Ms, policies, and evidence lists.



Secure partner collaboration

Collaborate with primes, suppliers, and partners in a controlled environment with stronger governance.



Less internal IT burden

Exostar manages platform operations so teams don't need to build and maintain compliant infrastructure.



Expert support where it matters

Professional services address gap analysis, remediation planning, and evidence review that software can't fully automate.

When CMMC Ready Suite™ makes sense

CMMC Ready Suite™ is ideal for organizations that:

- Handle or expect to handle CUI
- Support DoD contracts or subcontracting relationships
- Want to reduce CUI exposure across corporate systems
- Need help generating SSPs, POA&Ms, and policies
- Want a more predictable path to readiness
- Need to prepare for CMMC Level 2
- Need to collaborate securely with partners and suppliers
- Do not want to build their own GCC High environment
- Have limited internal cybersecurity or compliance resources
- Need both technology and services support

Aligned to your readiness needs

Every organization's CMMC journey is shaped by how CUI moves through the business: where it lives, who needs access, how it is shared, and whether it must be exchanged across teams and partners. Exostar's CMMC Ready Suite™ is a flexible technology + services model that aligns to the customer's actual CUI use case and readiness complexity.

TECHNOLOGY

Technology packages

Based on number of users

01

Up to 10 users

Same secure technology stack, sized for small teams

02

Up to 20 users

Same secure technology stack, sized for growing teams

03

Up to 50 users

Same secure technology stack, sized for larger organizations

SERVICES

Professional services packages

Based on CUI scope and complexity

01

Simple CUI data flow

All CUI stored, processed, and transmitted within the Exostar solution

02

Defined external data flows

Small organizations with one or two CUI data flows outside the enclave

03

Complex, multi-site scope

In-depth engagement: scoping how CUI moves, training, assessment, remediation, and support

Technology tiers share the same secure stack and differ only by user count. Services tiers scale with how far CUI travels: entirely inside the Exostar solution, through a few defined external flows, or across a complex multi-location organization.

How Exostar recommends the right package

Exostar recommends the right combination of technology and services based on the customer's CUI workflows, scope complexity, readiness maturity, internal resources, and assessment timeline. The goal is to help customers understand why CMMC complexity affects scope, effort, and cost — without forcing them to overbuy or navigate the process alone.

Customers don't have to guess which tools or services they need.

Exostar recommends the right package based on how CUI is actually handled, how complex the scope boundary is, and how much support the team needs to prepare for CMMC Level 2 readiness.

Why Exostar for CMMC readiness

Exostar is a trusted partner for organizations operating in highly regulated industries and complex partner ecosystems. With deep experience supporting the Defense Industrial Base, Exostar delivers purpose-built solutions that help organizations collaborate securely, manage identity and access, and simplify compliance.



Built for the Defense Industrial Base

Deep experience in regulated industries and complex partner ecosystems — secure collaboration, identity and access, and simplified compliance.



One readiness-focused solution

Secure collaboration, identity, compliance automation, documentation and policy generation, and professional services — coordinated, not stitched together.



Faster, with less to build

Move toward CMMC Level 2 readiness with lower total cost of ownership and no compliant environment to build and run in-house.

Ready when you are.

When organizations are ready to begin their CMMC readiness journey, Exostar is ready to support them with the right technology, services, and guidance to help them succeed.



THE BOTTOM LINE

A tangible, defensible path to CMMC readiness

Exostar's CMMC Ready Suite™ gives Defense Industrial Base organizations a tangible, defensible path by combining the technology needed to protect CUI with the services needed to close gaps, organize documentation, and support ongoing self-assessments and affirmations.

With tiered technology and services, Exostar helps customers align the right package to their CUI workflows, scope complexity, readiness gaps, and internal resources — without overbuying or navigating the journey alone.

Talk to Exostar →