eSHARE

The State of CMMC Compliance in 2025

Trusted Collaboration Inside M365 GCC

What is CMMC?

CMMC 2.0 compliance for Defense Industrial Base (DIB) contractors now is at risk whenever they can't control their CUI data. The moment CUI is shared outside their boundary they become liable for their partners' security postures.

This "flow-down" liability is the primary focus of DIBCAC assessors, and most tools—including popular secure portals—can't prevent it. Microsoft 365 GCC High is the only Microsoft cloud environment approved for ITAR and export-controlled data. But alone, it's not enough. Once a partner decrypts CUI on an uncontrolled device, your CMMC boundary is broken— and your status is at risk.

eSHARE solves this by keeping files inside your Microsoft 365 GCC High boundary.

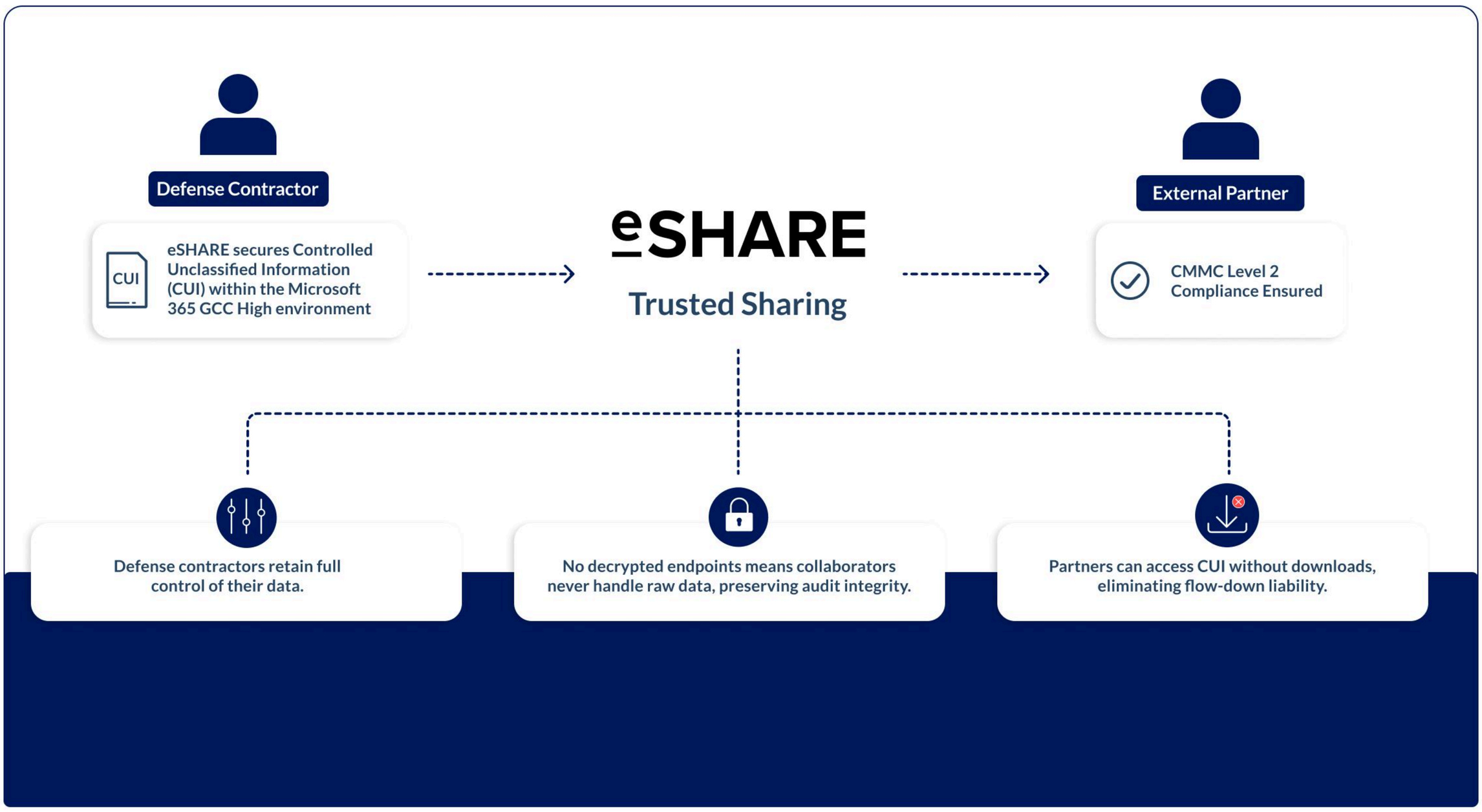
NO DOWNLOADS

NO DECRYPTED ENDPOINTS

NO FLOW - DOWN RISK

The strategic decision to adopt Microsoft 365 GCC High was the correct one—it is the only Microsoft cloud environment authorized for ITAR and other export-controlled data. However, the platform alone does not solve the DIB's most critical compliance vulnerability: the moment a collaborator downloads and decrypts CUI, their non-FIPS-140-validated endpoint shatters your CMMC boundary and creates an indefensible audit failure.

Legacy tools and partial solutions force DIB contractors into a "Frankenstein system" of bolted-on technologies that fail to address this core problem. This paper details how eSHARE provides a fundamentally different architecture, activating your GCC High investment to deliver the complete foundation for 100% of CMMC Level 2 controls and providing the verifiable proof needed to pass your audit with confidence.



The Architectural Flaw of Legacy Security in a CMMC Audit

Traditional methods for sharing CUI—including encrypted email, SFTP, and even modern “secure” file-sharing portals—are misaligned with CMMC requirements. They’re all built to move data out of your environment, not keep it under your control.

An auditor must "determine if" and "verify that" CUI flow is controlled. When a file leaves your GCC High tenant, you can no longer provide objective evidence to satisfy this objective. You lose control, and you inherit the compliance risk of your partner's environment. This forces a choice between mission-critical collaboration and compliance.

eSHARE's Solution:

Containing the Boundary to Eliminate the Risk

eSHARE creates a temporary, secure sandbox inside your GCC High tenant in which to securely collaborate. External partners can work on CUI in real time—but the file itself the data never leaves your secure perimeter.

Our Trusted Shares™ use Microsoft Service Principals to build ephemeral, FIPS 140-2 validated containers that enforce Zero Trust from start to finish.

NO GUEST ACCOUNTS

NO DATA LEAKAGE

FULL CONTINUOUS AUDITING

This is the complete foundation: Microsoft 365 GCC High + eSHARE. Our customers are leveraging this two-part solution to achieve 100% of CMMC Level 2 controls and pass their audits with perfect scores.

Satisfying CMMC Level 2 Assessment Objectives with eSHARE

eSHARE is an evidence-generation platform, designed to provide auditors with the definitive proof needed to verify your compliance. Our Trusted Shares™ use Microsoft Service Principals to build ephemeral, FIPS 140-2 validated containers that enforce Zero Trust from start to finish.

CMMC Requirement	eSHARE Alignment with CMMC Requirements
CMMC Requirement (What an Auditor Needs to Verify)	eSHARE's Verifiable Proof & Architectural Advantage
Prove complete control over CUI flow	eSHARE's Trusted Shares™ prevent decryption on external devices, providing objective evidence that your CMMC boundary is never breached.. Our Outlook integration transparently converts risky attachments into secure, in-tenant links, closing your most common data spillage vector and providing an auditable record of a controlled workflow.
Maintaining FIPS-Validated Cryptography	Our architecture ensures that the FIPS 140-2 validation of your GCC High tenant is never compromised. Since CUI is never decrypted on an external device, you can definitively prove to an assessor that data is protected by validated cryptography throughout its entire lifecycle.
Deliver Irrefutable Proof of User Actions	We deliver an immutable, forensic-quality audit trail for every collaborative session. Our logs provide the definitive evidence an auditor needs to "uniquely trace the actions of individual users. eSHARE generates a forensic-quality audit trail that uniquely traces every action—from creation to deletion—to an individual user, satisfying the entire AU domain.
Managing Supply Chain Risk	eSHARE fundamentally solves the flow-down liability problem. By containing collaboration within your own tenant, you no longer inherit the compliance risk of your partners' environments. You can enable your supply chain without being liable for their security posture.

The Path to a Defensible Audit

Partial compliance is failed compliance. Legacy tools create complexity, risk, and audit gaps.

With eSHARE, the path to a successful CMMC audit with irrefutable proof is made simpler. By enhancing your Microsoft 365 GCC High tenant with Trusted Collaboration, you get a single, integrated solution for continuous governance with 100% of required Level 2 controls.

Schedule a demo to see how eSHARE delivers what assessors demand.

About eSHARE

Get in touch to find out how eSHARE can enhance your security framework and redefine the way you collaborate.

Linkedin
info@eshare.com
www.eshare.com