Supporting CMMC Level 2 with Data-Centric Security

Virtru for Email, Virtru Secure Share, and Virtru Private Keystore

Aligned to CMMC FAQ Rev 2.2 (Jan 2026)

Executive Summary

CMMC Level 2 requires defense contractors to protect Controlled Unclassified Information (CUI) wherever it is processed, stored, or transmitted, including when it leaves traditional network or enclave boundaries.

Virtru enables **secure sharing of CUI outside the enclave** while maintaining strong **scope control**, by combining:

FedRAMP Moderate authorized cloud services

Data-centric, end-to-end encryption

Split-knowledge (Zero Trust) architecture

This approach aligns directly with recent DoD guidance clarifying how encryption, enclaves, and external services affect CMMC scope.

Key DoD Clarifications in CMMC FAQ Rev 2.2

Recent guidance reinforces four principles relevant to CUI data flows, including email and file sharing:

Encrypted CUI remains CUI — encryption does not de-control data, so encrypted CUI remains in scope for CMMC assessment.

Encryption alone does not create logical separation. The CMMC Level 2 scoping guide provides detail on what it considers "logical separation," using software or network assets to separate in-scope systems and assets from out-of-scope systems and assets. Just because CUI is encrypted, doesn't mean it's excluded from the scope of your assessment. You need to demonstrate adequate protections for CUI at all times, even when encrypted.

Properly encrypted CUI may traverse out-of-scope systems *when logical separation exists.* Logical separation — such as access control, key management, and policy enforcement — is necessary to safeguard encrypted CUI. Only then can encrypted CUI traverse or reside in systems that are otherwise out-of-scope for compliance.

Cloud services storing CUI must meet FedRAMP Moderate or equivalency requirements. Note that, if choosing a FedRAMP equivalent vendor rather than a FedRAMP authorized vendor, you bear additional reporting responsibilities in case of a breach.

Virtru's architecture is designed to meet these expectations **by design**, not by exception.

Secure CUI Sharing Without Expanding Scope

Powered by the Trusted Data Format, Virtru creates a secure container for CUI, enabling it to be shared with external contractors or government agencies without sacrificing security or compliance.

FedRAMP Moderate Authorized Cloud

Virtru is **FedRAMP Authorized at the Moderate level.**

When customers use Virtru for Email or Virtru Secure Share:

- **Encrypted CUI files are stored in Virtru's FedRAMP Moderate authorized cloud**
- This satisfies **DFARS 252.204-7012** and **CMMC FAQ Section E** requirements for cloud services that store or transmit CUI
- Customers do **not** need to implement separate FedRAMP controls for Virtru's environment

Split-Knowledge (Zero-Trust) Architecture

Although Virtru stores **encrypted CUI** in its FedRAMP-authorized cloud:

- **Virtru cannot access customers' CUI,** because the encryption keys are managed separately from the content.
- Encryption keys are controlled by the customer (or customer-managed key service).
- Virtru cannot decrypt, view, or access plaintext CUI.

What this means for CMMC

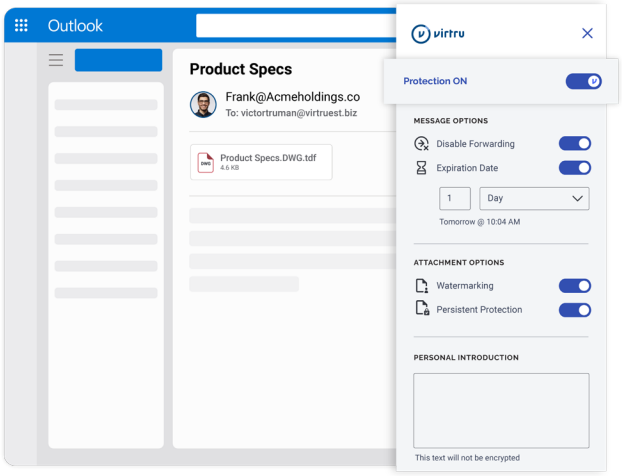
- Virtru functions as a **secure, compliant storage and transmission layer for files containing CUI.**
- CUI remains unusable to Virtru personnel or systems
- Risk is reduced without introducing uncontrolled third-party access

---

Sharing CUI Via Email Attachments with Virtru

How It Works

- When a secure email is composed, CUI is encrypted and stored in Virtru's FedRAMP Moderate cloud.
- Access is enforced through identity-based policy: Recipients must authenticate with their Google or Microsoft credentials.
- Encrypted content may reside in Virtru's FedRAMP Moderate cloud, but it remains inaccessible without authorization.



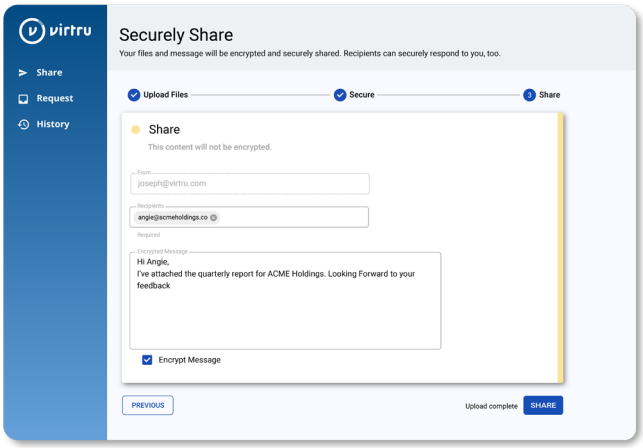
CMMC Level 2 Value

- Protects CUI during transmission and storage.
- Prevents uncontrolled dissemination via inboxes or forwarding.
- Supports SSP statements that clearly define **where CUI is readable vs. encrypted-only.**
- Aligns with NIST SP 800-171 controls across **AC, IA, SC, and MP** (Access Control, Identification and Authentication, System and Communications Protection, and Media Protection).

Sending and Receiving CUI with Virtru Secure Share

How It Works

- Files are encrypted individually upon upload
- Access is provided through a secure viewer or controlled download
- Encrypted files are stored in Virtru's FedRAMP Moderate cloud
- Access can be revoked, audited, or time-limited at any time, under the data owner's control



CMMC Level 2 Value

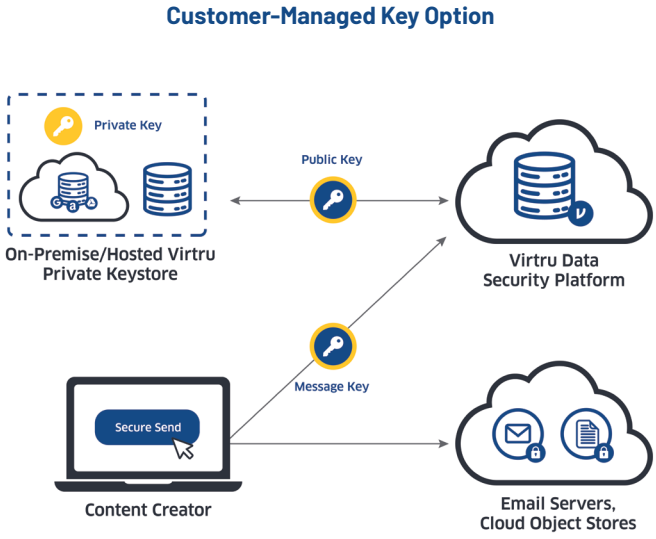
- Enables secure collaboration without bringing partner systems into scope
- Supports enclave-based architectures validated in Rev 2.2 guidance
- Keeps CUI encrypted and unusable outside authorized sessions

---

Shielding CUI from Cloud Service Providers with Virtru Private Keystore

How It Works

- For an additional layer of control over encrypted CUI, host your private encryption keys
- Store in the location of your choice — on-prem, HSM, or cloud (public or private)
- Strengthen privacy by ensuring any request to access data (including a government subpoena) has to come to your organization — not through your cloud provider or any other third party.



CMMC Level 2 Value

- Demonstrates heightened control of encrypted CUI
- Ensures CUI is inaccessible to cloud providers, with keys physically and logically separated from content
- Supports enclave-based architectures validated in Rev 2.2 guidance

CMMC Level 2 Alignment at a Glance

Requirement Area	Virtru Support
FedRAMP Moderate CSP	Virtru cloud is FedRAMP Authorized (Moderate)
Protection of CUI at rest & in transit	Data-centric encryption at the object level
Third-party access risk	Split-knowledge / Zero Trust design
Scope control	CUI remains unusable on out-of-scope systems
SSP clarity	Clear articulation of encrypted-only storage locations
Assessment defensibility	Architecture aligns with Rev 2.2 FAQ guidance

See why defense contractors trust Virtru to protect CUI.
Book a demo today at virtru.com.