Safeguard CUI to Strengthen CMMC 2.0 Compliance

Apply Data-Centric Security with Virtru

Data-Centric Security for CMMC 2.0

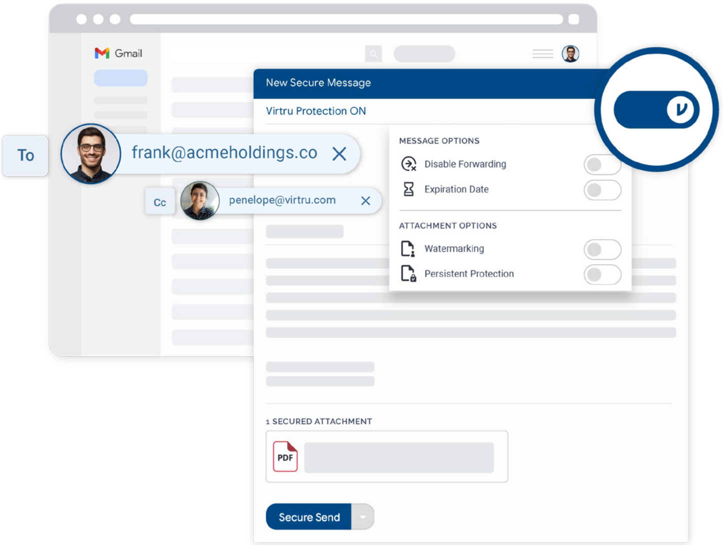
As the rollout of the Cybersecurity Maturity CMMC 2.0 continues, contractors that handle controlled, unclassified information (CUI) need to implement safeguards for covered defense information from DFARS 252.204-7012 and meet requirements within NIST SP 800-171 for protecting the confidentiality of CUI in nonfederal systems. But many collaboration workflows put CUI's confidentiality at risk, especially in cloud environments.

Virtru helps streamline your organization's preparations by protecting CUI from unauthorized access, without limiting your ability to share it with designated contacts. With easy-to-use, end-to-end encryption and key management solutions that support NIST and DFARS requirements for protecting CUI, Virtru supports key CMMC practices and processes while enabling secure sharing and collaboration.

Protect CUI Without Sacrificing Collaboration

WIth Virtru, your teams can collaborate quickly and securely in the apps they already use every day.

- **Client-Side Encryption for Email and Files:** With Virtru for Google Workspace and Microsoft 365, your teams can work inside the apps they already use every day, with a simple toggle button to encrypt and apply granular access controls to shared CUI.
- **Server-Side Data Control:** Detect and automatically enforce encryption for sensitive information being shared.
- **Secure File Intake:** Securely collect documentation in a single location with Virtru Secure Share, which encrypts data upon upload.



Virtru for Gmail: Client-Side Data Control

- **Control Your Own Encryption Keys for Data Sovereignty**: The Virtru Private Keystore allows you to host your keys wherever you like: a public or private cloud, private or co-hosted data center, or HSM.

Strengthen CMMC 2.0 Readiness and Secure the Defense Supply Chain

Keep CUI Confidential: Protect CUI's confidentiality to meet NIST, DFARS, and CMMC requirements for access control, audit and accountability, integrity, and protections for media, systems, and communications.

Shield Your Data: With the Virtru Private Keystore, encryption keys can be stored separately from cloud-hosted data in on-premise, cloud, or third-party-hosted key servers — meaning neither Virtru nor your cloud provider can view your data.

Empower Secure Sharing: Enable seamless, secure CUI sharing throughout contracting and supply chain collaboration workflows, while maintaining persistent control and visibility.

Unlock Collaboration Workflows: Equip primes, subcontractors, and mission partners to share information quickly and securely, powering innovation throughout the defense industrial base to drive growth.

Tie Identity to Data Access Decisions: The Virtru Data Security Platform integrates with in-place organizational identity management systems, such as PKI, OAuth, Active Directory, and LDAP.

Strategically Tag Information: Apply discrete data tags that are bound to the content itself, connected with attribute-based access control (ABAC) policies and rules.

Trusted by Over 7,000 Customers for Data-Centric Security, Privacy, and Compliance

omada CapitalOne Tower Semiconductor Berkeley UNIVERSITY OF CALIFORNIA

virtru

See how Virtru can equip your organization with data-centric security for CMMC 2.0: Book a demo at **virtru.com/contact-us**