

Protect CUI Everywhere It's Shared to Prepare for CMMC

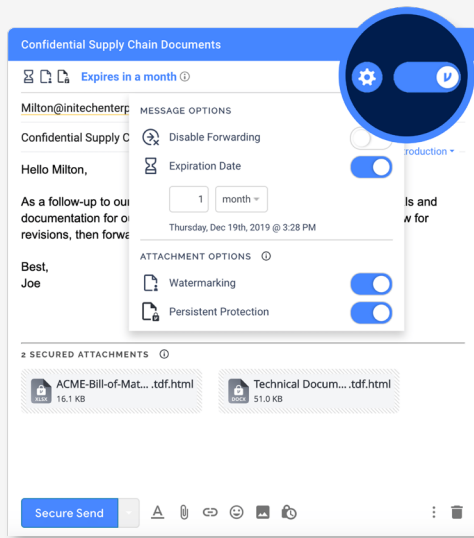
Virtru protects controlled unclassified information (CUI) from unauthorized access to prepare your organization for Cybersecurity Maturity Model Certification (CMMC) Level 3 Maturity.

Virtru Positions Your Organization for CMMC Level 3

As CMMC begins its phased rollout, defense contractors that handle CUI need to achieve Level 3 Maturity by implementing safeguards from DFARS 252.204-7012 related to data protection and access controls for CUI within NIST SP 800-71. Yet collaboration workflows risk the exposure of CUI to unauthorized users, especially in cloud environments.

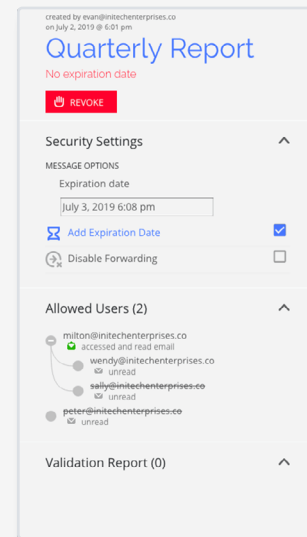
Virtru helps streamline your organization's preparations for Level 3 Maturity by protecting CUI from unauthorized access everywhere it's shared. With easy end-to-end email and file encryption, Virtru supports key CMMC practices and processes for Level 3 Maturity while enabling secure sharing and collaboration workflows that power innovation and growth.

Data Protection and Control to Prevent Unauthorized Access to CUI



End-to-End Encryption & Persistent Control

Protect Gmail, Drive, and Outlook with end-to-end encryption that prevents unauthorized access to CUI stored in the cloud and shared throughout the supply chain. Disable forwarding, set expiration, and revoke access. Watermark files to deter leaks, and maintain persistent control wherever files are shared.



Granular Audit Trails

View when and where email messages and files containing CUI have been accessed throughout digital sharing workflows, and adapt controls for evolving supply chain requirements.

Unlock Defense Supply Chain Workflows with Secure CUI Sharing



CUI Protection

Protect CUI from unauthorized access to meet CMMC requirements for access control, audit and accountability, integrity, and protections for media, systems, and communications.



Secure Sharing

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



Innovation & Growth

Unlock new collaboration workflows between primes, subcontractors, and mission partners, powering innovation throughout the defense industrial base to drive growth.

Proven Platform to Support Privacy and Compliance



Trusted Data Format (TDF)

Open data protection standard for object-level encryption. Virtru solutions use the TDF to bind encrypted data to policies and metadata, ensuring only authorized users can access CUI.



Software Development Kit (SDK)

Embed CUI protection and control into the apps and systems that power your digital supply chain workflows to prevent unauthorized access.



Key Management

Integrate with existing key management processes and Hardware Security Modules (HSMs). Host your own keys so that only your authorized users can access the keys protecting CUI.

More than 20,000 Organizations Rely on Virtru to Unlock the Power of Their Data



Learn how Virtru can help fast-track your CMMC preparations today: virtru.com/contact-us