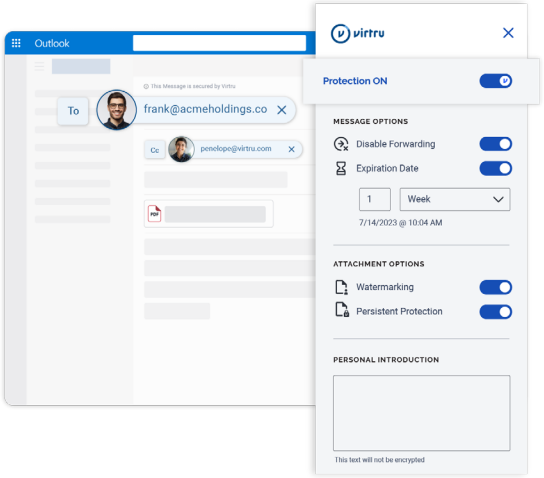
FedRAMP Authorized, Data-Centric Security for CMMC

Protect and share CUI without breaking the bank

Virtru strengthens your CMMC compliance posture by protecting CUI from unauthorized access, without limiting your ability to share it with designated contacts. Virtru is easy to use, with FedRAMP authorized, FIPS 140-2-validated, 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.



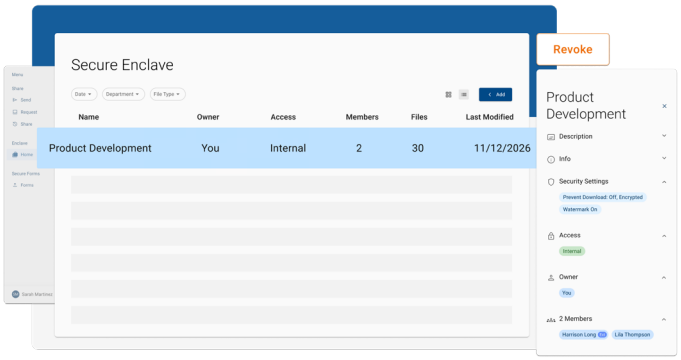
Virtru for Microsoft Outlook

Powered by the open-standard Trusted Data Format (TDF), Virtru's solutions bring object-level security and governance to enterprise data. Virtru integrates into the workflows you interact with most, including email, file sharing, and file storage. The TDF binds security policies directly to individual data objects (like project files, design specs, or personnel details), creating a protective wrapper that travels with your data wherever it goes, allowing for persistent protection with granular visibility, control, and audit.

Protect CUI Without Sacrificing Collaboration

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

- **FedRAMP Authorized File Storage and Sharing:** Securely collect, store, organize, and share files with Virtru Secure Share and Secure Share Enclave.
- **Client-Side Encryption for Email and Files:** With Virtru for Google Workspace and Microsoft 365 Commercial Cloud, your teams can work inside the apps they already use every day, with a simple extension and toggle button.
- **Advanced Security Rules & Audit:** Detect and automatically warn or enforce encryption for sensitive information being shared. Audit your CUI wherever it travels.



Virtru Secure Share Enclave

- **Easy to Use**: Deploy in minutes, with no new tenants, mailboxes, or gateways. Recipients seamlessly decrypt using the Virtru Secure Reader with their existing credentials: No new usernames, passwords, or accounts.

©Virtru Corporation. All rights reserved.

Strengthen CMMC Readiness and Secure the Defense Supply Chain

Keep CUI Confidential: Protect CUI 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 optional 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. Virtru also supports Google CSE as a trusted external key vendor.

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.

Find Trusted Partners: Access the Virtru Trust Center to learn more about our standards, and explore the Virtru Compliance Champions Program for access to our community of trusted CMMC advisors.

Trusted by Over 6,100 Global Customers
Proven through L2 C3PAO Assessments

JD MACHINE Advanced Manufacturing

salesforce

Maya HTT

NC STATE UNIVERSITY

virtru

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

©Virtru Corporation. All rights reserved.