Virtru for Defense

Mission-Critical Data Protection for Federal Agencies and Partners

Data protection has always been critical to enabling Federal missions and improving the delivery of services to stakeholders who depend on them. Now, advances in technology bring massive opportunities for rapid collaboration and more informed decision-making, but also introduce new risks.

Virtru's persistent data protection and granular access control capabilities empower government agencies and partners to streamline collaboration, unlock the power of data, and maintain control, wherever it is shared. Using Virtru, you can:

- Use encryption and attribute-based access control to share sensitive data with other departments, mission partners, and the supply chain.
- Ensure compliance and alignment with regulations and standards such as CJIS, CMMC, FedRAMP, ITAR, NIST, and more.
- Use implementations like protected email and encrypted files for office productivity or secure analytics and low overhead IoT data protection to enable mission success.
- Unlock digital workflows to support remote workers and distributed teams.
- Boost user adoption with easy-to-use protections, seamless recipient access, and a quick installation process that gets users up and running in minutes.

Unlock Compliant, Mission-Critical Workflows

Confidentiality & Compliance

End-to-end encryption prevents unauthorized access to sensitive data to maintain the confidentiality of protected data and meet compliance requirements.

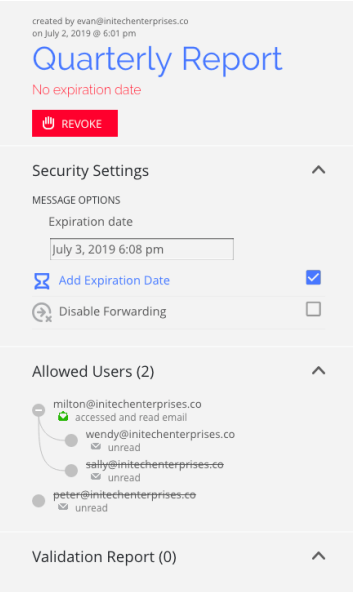
Secure Sharing

As sensitive data is shared across networks, cloud environments, and devices, Virtru keeps it secure with persistent protection and lets you govern access throughout the data lifecycle.

Ease of Use

Virtru's seamless user experience ensures broad adoption with minimal IT overhead. End-to-end encryption and access controls are embedded where users, admins, and partners already work.

Keep Sensitive Data Protected and Under Your Control, Wherever It's Shared



Persistent Protection: Protect classified and controlled unclassified information (CUI) with the open standard Trusted Data Format (TDF), approved for use by the Office of the Director of National Intelligence (ODNI).

Attribute-Based Access Controls: Enable secure sharing across agencies with attribute-based access controls (ABAC) for sensitive data. Control data wherever it's shared with instant access revocation, expiration, disable forwarding, and document watermarking capabilities.

Granular Audit and SIEM Integrations: View who has accessed protected data, when, where, and for how long to streamline audits and support compliance reporting. Integrate data logs with your SIEM for advanced threat analysis and incident response workflows.

Key Management: Host your own keys for full control, or let Virtru host your keys and manage access policies and key requests. Integrate with Hardware Security Module (HSM) devices supporting PCKS#11 and KMIP for the highest security assurances.

Federal Compliance Certifications

FedRAMP

Virtru has a certified Authorization to Operate (ATO) at the moderate level under FedRAMP. As part of our FedRAMP compliance program, we adhere to the security controls defined in the NIST 800-53 and 800-171 publications to ensure the integrity of federal information systems.

AICPA SOC

Virtru's security operations and processes are validated by third-party assessments for Service Organizations Control (SOC) 2 Type 2 Compliance. This attests that we can be trusted to safeguard sensitive customer data in the cloud.

Trusted by Federal Agencies, Mission Partners, and Thousands of Other Organizations

NIST

CDC Centers for Disease Control and Prevention

virtru Learn more at virtru.com/federal-government