Virtru for Government

Easily Protect Confidential, Mission-Critical Data, Wherever It’s Created or Shared

Every organization has applications and processes that share sensitive data, whether employee or machine generated. This requires a layered solution to confidently manage data sharing as the amount of generated data grows and requirements to protect data evolve. The Virtru Data Protection Gateway automatically protects data shared by custom internal applications or enterprise SaaS applications and integrates with your existing email infrastructure and workflows to provide data protection when and where it’s needed.

Inbound + Outbound Protection for Data Security, Collaboration, and Control

Encryption, Decryption, and Policy Enforcement for Data Sharing Workflows

- Protect messages sent and received by custom or SaaS applications like Salesforce, Zendesk, and Workday, without disrupting existing processes.
- Enforce DLP policies by scanning messages and attachments for sensitive data and adding encryption and access controls.
- Enable seamless recipient access and response workflows, without requiring new accounts, passwords, or software.
- Support rapid time-to-value and reduce IT overhead with Virtru and cloud-hosted deployment options and mail flow integrations.

“Virtru Data Protection Gateway has been a game changer for our organization, giving power back to our security team while not inhibiting our users. Deployment went incredibly smoothly, fitting seamlessly with our existing workflows while automatically protecting data organization-wide.”

- Charles Brehm, IT Manager, Service Coordination, Inc.
Hosting Options and Deployment

- **Virtru Managed** - Meets most common data protection needs by offering outbound encryption and inbound decryption with a seamless deployment process.

- **Customer (Self) Managed** - Offers added functionality to meet additional requirements by hosting on your cloud provider such as AWS, Azure, or Google Cloud platforms or on-premise.

Outbound Encryption protects emails and files before they leave your domain to ensure communications stay compliant, private, and secure.

Outbound Decryption and Archiving allow emails to be copied and sent to archives to support eDiscovery and audit reporting processes.

Outbound Data Loss Prevention determines what messages get auto-encrypted based on security policies, what can pass without requiring encryption, and what warns (or logs) a potential issue.

Inbound Encryption secures PII and PHI within incoming messages sent from patients, customers, clients, and partners, to ensure compliance.

Inbound Decryption enables plaintext scanning by an application or MTA (Mail Transfer Agent) before it enters your domain for anti-malware, anti-spam, and compliance.

Supported Workflows

See Virtru in action. Contact us today at virtru.com/contact-us.