Virtru Data Protection

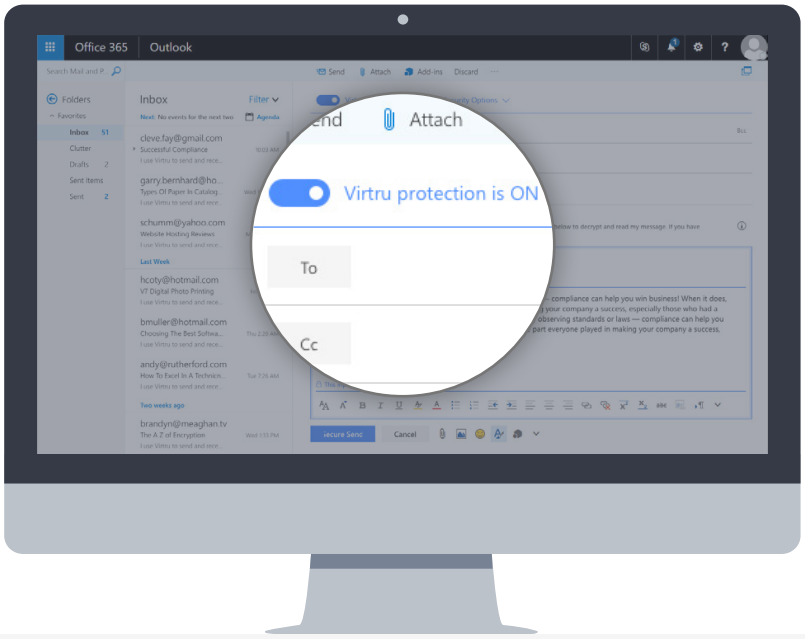
Email Encryption, Access Control, and Monitoring for Federal Agencies

Government agencies need an easy way to protect, share, and manage access to sensitive data. Trusted by federal agencies, state and local governments, and thousands of other organizations, Virtru offers seamless email protection and control that eliminates the pain of legacy encryption solutions.

Protect from Creator to Consumer
One click secures content from creation to consumption for complete, end-to-end protection.

Share with Anyone on Any Device
Recipients can access protected content regardless of their technology, without creating new accounts.

Control Information Wherever It Travels
Revoke, expire, and track or disable forwarding – even after content has been read.



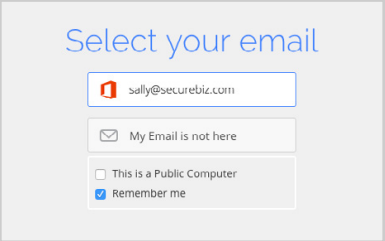
More Than 8,500 Organizations Trust Virtru's Data Protection Software

Maryland

"The great thing about Virtru is you don't have to download anything to be able to receive secure messages. You will receive these secure messages in the same way you receive other emails."

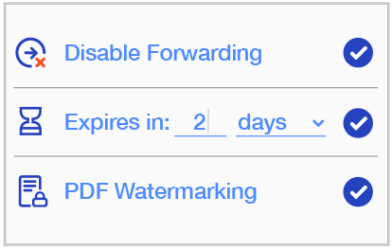
– Federal Healthcare Agency

A Closer Look at Virtru Email Encryption



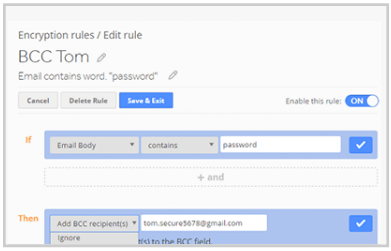
Easy Recipient Access and Collaboration

Never force external recipients to install new software or create new logins. Virtru uses existing applications, accounts, and credentials.



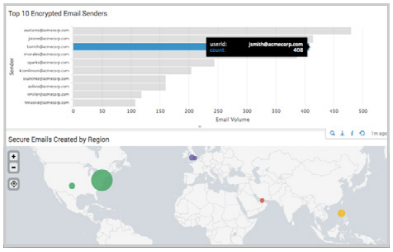
Powerful Internal and External Access Controls

Revoke messages, set expiration, control forwarding, and watermark PDFs. Access controls also prevent unauthorized insider sharing between employees.



Painless Administration and Policy Enforcement

Rapid enterprise deployments for quick time to value. Virtru Control Center gives admins centralized DLP policy management and granular reporting.



Granular Audit, SIEM Integration, and Incident Response

Stop data leaks by auditing who encrypts, shares, and accesses protected content, directly from within the agencies SIEM.

Flexible, Enterprise-Grade Key Management

- Host and manage encryption keys on-premise for absolute control and privacy.
- Deploy rapidly across the agency with Docker containers that support scalable, agile, and secure IT infrastructure.
- Integrate with Hardware Security Module (HSM) devices supporting the PCKS#11 standard and KMIP protocol for the highest level of security.

Zero Trust Security

- Virtru's zero trust model ensures only authorized parties can access email content.
- Split knowledge architecture separates encryption keys from the content, so you're never forced to trust Virtru or your email provider with access to your data.

Federal Compliance Certifications

We strive to meet federal requirements for keeping data secure, wherever it travels.

FedRAMP

We're in process for FedRAMP authorization at the moderate baseline, with full Authorization to Operate (ATO) expected in Fall 2018. As part of our FedRAMP compliance program, we adhere to controls defined in NIST 800-53 and 800-171.

AICPA SOC 2

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.

virtru