Virtru Data Protection Gateway

virtru
RESPECT THE DATA

Protect data before it leaves or enters your network, while maintaining complete control and visibility.

Organizations face security challenges as sensitive data flows through email and SaaS applications, often unprotected. Traditional security approaches require users to change their behavior or learn new tools, leading to adoption issues, security gaps, and disruptions. The Virtru Data Protection Gateway delivers data protection across your domain using targeted security rules —seamlessly identifying and encrypting sensitive information shared via email and SaaS applications without user intervention.

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

Private, Secure Sharing

Automatically protect internal and external sharing workflows, protect confidentiality, and help prevent human error.

Data Security and Compliance

Maintain support for data privacy regulatory compliance obligations such as HIPAA, GDPR, PCI, and CCPA.

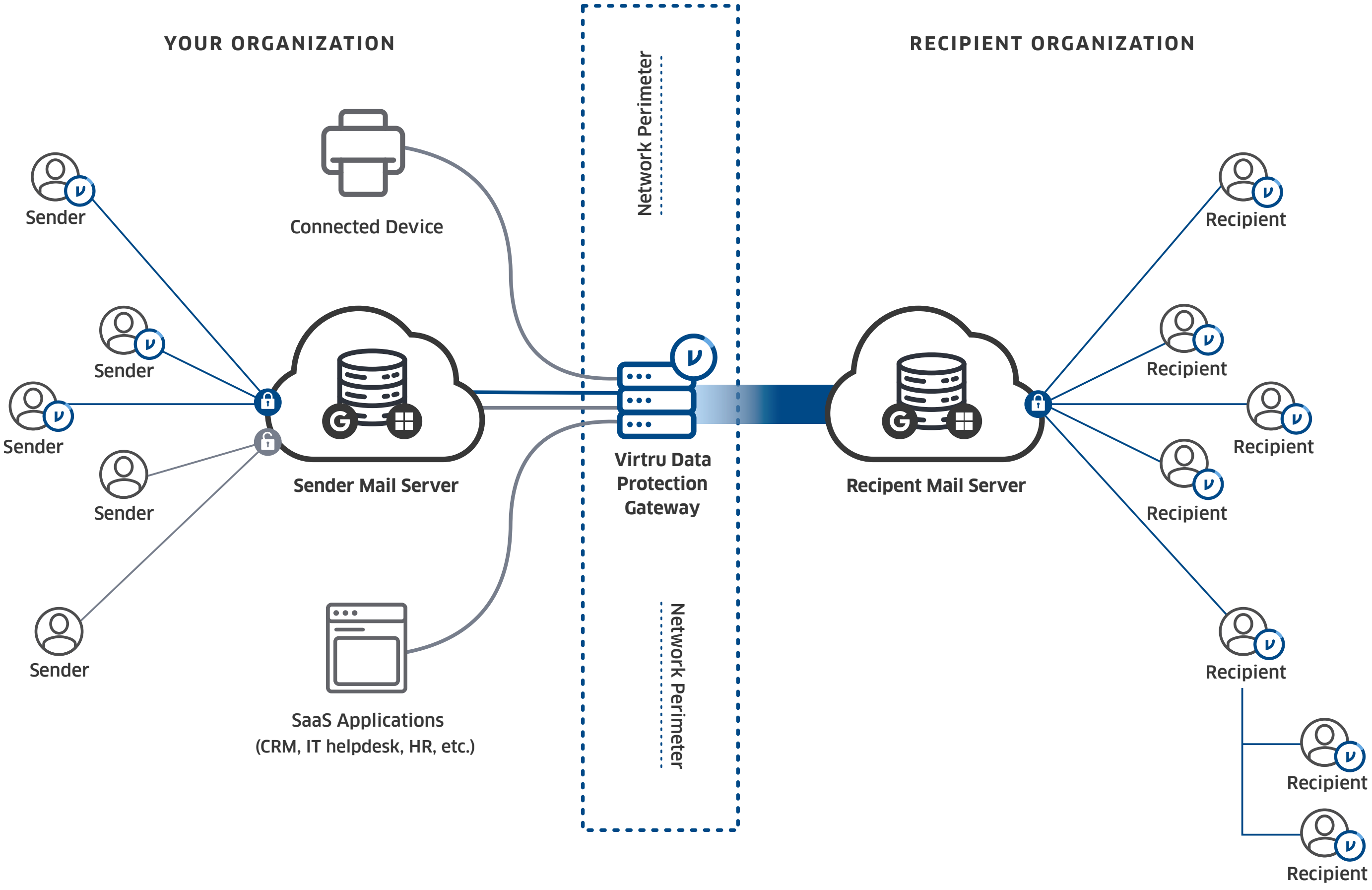
Efficient Workflows

Targeted encryption accurately protects sensitive data flowing in and out of your organization to maintain efficiency without compromising security.

Encryption, Decryption, and Policy Enforcement for Data Sharing Workflows

- Automatically scan messages and attachments shared via email and SaaS applications to add encryption and access controls without disrupting existing workflows.
- Enable seamless recipient access and response workflows, without requiring new accounts, passwords, or software.
- Advanced analytics provide insights into email activity and how sensitive data is shared across the organization to help you make informed security decisions.

> *"The 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.



Supported Workflows

- **Outbound Encryption** protects emails and files before they leave your domain to ensure workflows remain efficient and secure.
- **Outbound Decryption and Archiving** allow emails to be copied and sent to archives to support eDiscovery and audit reporting processes.
- **Outbound Security Rules** determine 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 data within incoming messages sent from patients, customers, clients, and partners, to maintain support for regulatory compliance obligations.
- **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.
- **Inbound Security Rules** provides greater protection and control over the communications your customers, partners, and vendors can send to you.

Hosting Options and Deployment

Choose SaaS or self-managed hosting and deploy across your entire domain in hours, not weeks, with minimal IT overhead — ideal for organizations with limited security resources who need automated, enterprise-grade protection.

Select from two flexible hosting options:

- **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-premises.

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