virtru

5 Ways Portal-Based Email Encryption is Failing You

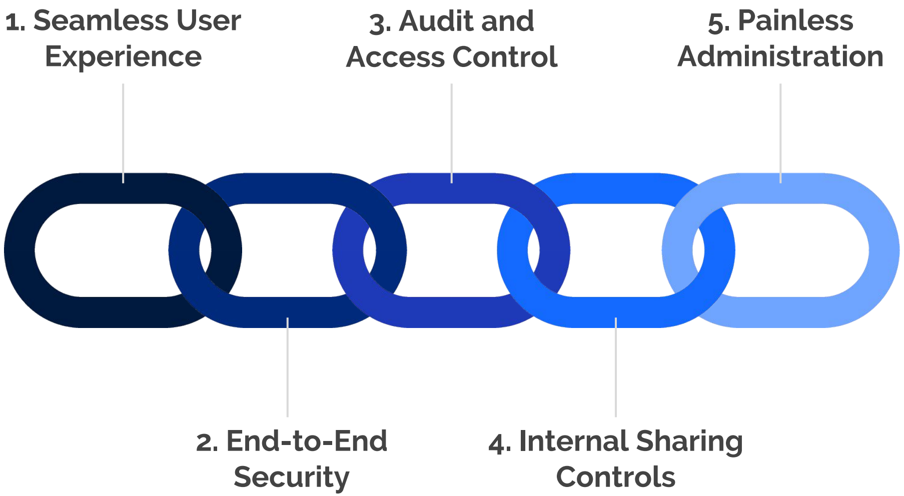
Portal-based Encryption Fails to Meet Modern Needs

Today’s enterprise is collaborative and cloud-centric, extending beyond clearly defined network perimeters. Email protections need to follow suit, yet portals and other perimeter-based approaches fail to align to the modern environment.

While enterprise technology, collaboration workflows, and threat vectors continue to evolve, legacy portal-based email protection technologies have not kept pace. Portal encryption solutions offer very limited access controls, add technical and administrative complexity, and burden end users with friction that hampers collaboration and efficiency.

Organizations must trade in perimeter-based security for data-centric security that shields the true target of data breaches. User experience, security, audit and access control, internal controls, and administration are all paramount concerns. They’re also crucial deficiencies of portal-based encryption approaches.

There are 5 key considerations for email encryption to meet modern enterprise requirements:

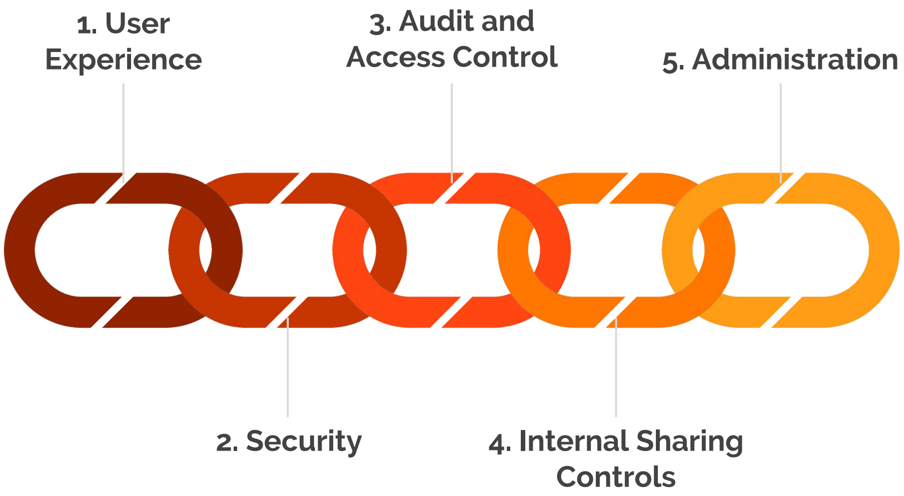

1. Seamless User Experience

2. End-to-End Security

3. Audit and Access Control

4. Internal Sharing Controls

5. Painless Administration



This paper highlights how portal-based email encryption comes up short in each category and fails to meet modern enterprise needs.

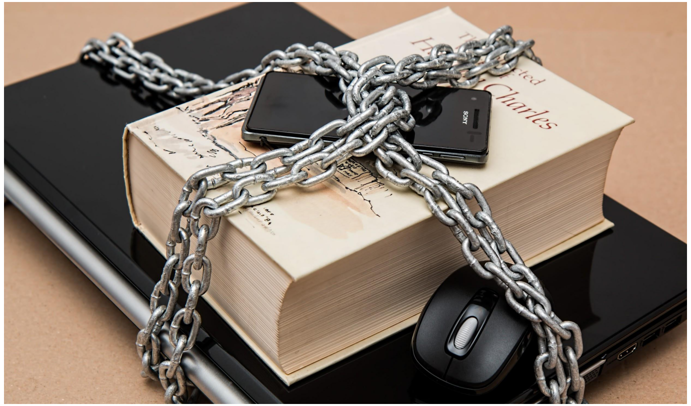
Portal Failure 1: **User Experience**

Portal-based technologies offer painful user experiences that thwart adoption. They make recipients manage new portal accounts and access email through a separate application. Due to weak customization features, portal emails often resemble phishing attacks, which ties up already overburdened helpdesks. And because portals lack easy on-demand encryption options and instead rely on hard-to-remember keywords, senders are forced into black box scenarios where they don't know if or how emails are protected.

This friction diminishes output and productivity, while encouraging savvy employees to find workarounds that introduce other security risks.

> "We had experience with a traditional, portal-based email encryption product, but we found this mechanism far too cumbersome for our users and their recipients."
>
> - **Mike Dieterich**, Director of Information Technology and Security, *Brown University*

Portal Failure 2: **Security**



Portals require you to place blind trust in the vendor securing unencrypted data. Sensitive messages are stored in the clear in the portal vendor's environment, And while your data sits unencrypted on the vendor's servers, it's only as secure as their network defenses, which puts your security completely in their hands.

Portals don't separate sensitive content from the encryption keys that secure it. This means unauthorized vendor employees or hackers could obtain the encryption keys then access your secure content. Since portals don't offer customer-controlled key options, they leave you blind to unauthorized third party access or government surveillance.

> "With other systems, encryption occurs after the message hits your email server. So, for a period of time, the content of that message and its attachments are exposed and vulnerable, and the draft and back-ups aren't protected either."
>
> - **Bill Dougherty**, Vice President of IT and Security, *Omada Health*

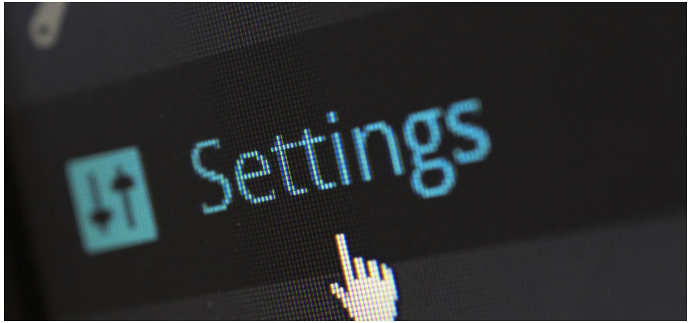
Portal Failure 3: **Audit and Access Control**

A major shortcoming of portal encryption technologies is their lack of comprehensive audit and access control features. Revocation, forwarding restrictions, expiration dates, and other controls are narrow, limited to a single platform, and unavailable to end-users.

As context around the data changes, the ability to adapt access privileges is rigid or absent. And without data-centric, object-level encryption, portals don't give admins clear visibility over their data, which weakens their ability to create a complete audit trail for analysis and compliance reporting.

> "With Zix's portal, we were never able to actually see if an email was secure — much less be able to revoke something sent in error."
>
> - **Ben Baez**, Application Administrator, *Bancroft*

Portal Failure 4: **Internal Sharing Controls**



Internal controls that prevent unauthorized insider access are virtually nonexistent with portals. The integrated DLP policies that they rely on only protect content shared externally. This perimeter-based approach does nothing to prevent employees from leaking confidential memos to other employees, which opens the door to internal employee relations crises.

The only way portals can prevent internal sharing is by forcing employees to go through the same painful external recipient user experience. This requires employees to use a redundant application and manage another account username and password to view email.

> "Most controls are designed to protect the data from external threats, leaving it vulnerable to careless or malicious insiders."
>
> - **Enterprise Security Operations Center Leader**

Portal Failure 5: **Administration**

Portal-based technologies create an excessive administrative burden that reduces time-to-value and compounds security risks. Portals exclusively rely on administrator-defined data loss prevention (DLP) policies. This requires admins to configure comprehensive rules and logic to detect sensitive content. This leads to excessive false positives that block harmless emails and slow down collaboration.

Since this process depends solely on the administrator's ability to dial in these controls just right, it centralizes risk and increases maintenance costs. Meanwhile, security awareness among end-users suffers.

> 61% of respondents cited solution complexity as the biggest inhibitor to security adoption and success, outpacing other factors by 3X.
>
> - **Enterprise Management Associates Survey, 2017**

Portal Encryption Failures Summarized

User Experience

Recipient friction, weak customization, black box security, and keywords make using portal encryption painful.

Security

Portal encryption security is not end-to-end and doesn’t give full control of encryption keys, requiring trust in third parties.

Audit and Access Control

Portals offer narrow, rigid DLP controls that aren’t available to end-users. Limited visibility into who has accessed content weakens audit capabilities.

Internal Sharing Controls

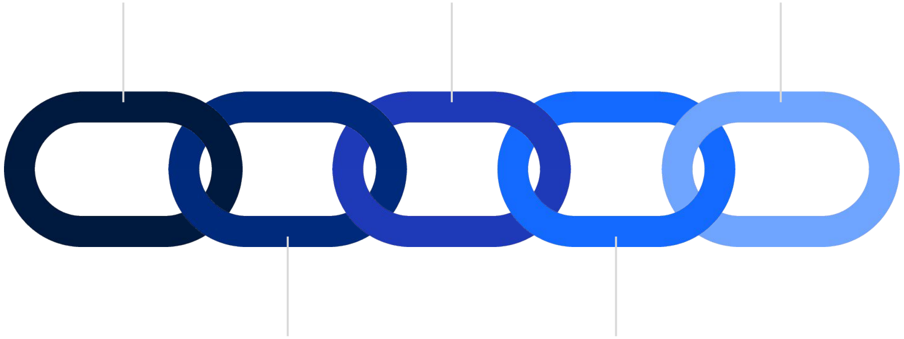
Portals don’t offer internal protections that prevent unauthorized sharing between insiders.

Administration

Portal encryption set-up and management is time-consuming and complex, and DLP relies completely on the administrator.

Virtru: Built to Overcome Portal Encryption Failures

In stark contrast to portal-based email encryption, Virtru offers the modern enterprise a new, easier, and more secure way to protect their email, making it as easy as possible for enterprises to protect their most sensitive content, share securely with anyone, and ensure the highest levels of confidentiality.



1. Seamless User Experience

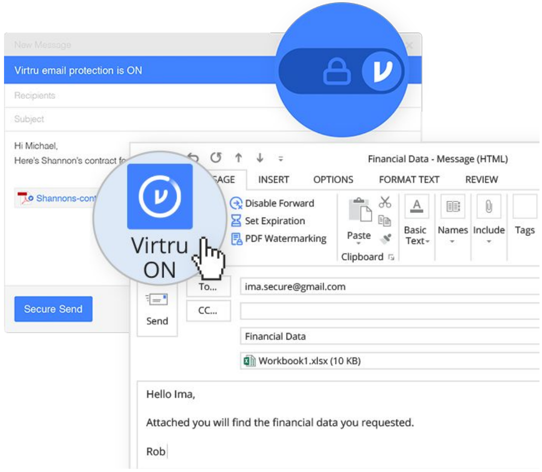
2. End-to-End Security

3. Easy Sharing with Anyone

4. See and Control Access to Emails and Files

5. Painless Administration

Virtru Offers Ease of Use, Audit, and Control



New Message

Virtru email protection is ON

Recipients

Subject

Hi Michael,
Here's Shannon's contract fo

Shannons-cont

Secure Send

Virtru ON

Financial Data - Message (HTML)

To... ima.secure@gmail.com

CC...

Financial Data

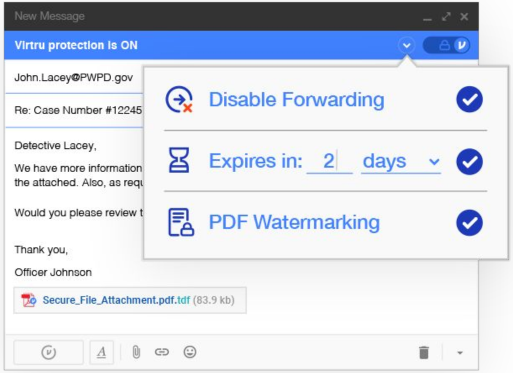
Workbook1.xlsx (10 KB)

Hello Ima,

Attached you will find the financial data you requested.

Rob

Seamless end-to-end encryption, on-demand and extremely easy to use.



New Message

Virtru protection is ON

John.Lacey@PWPD.gov

Re: Case Number #12245

Detective Lacey,

We have more information the attached. Also, as requ

Would you please review t

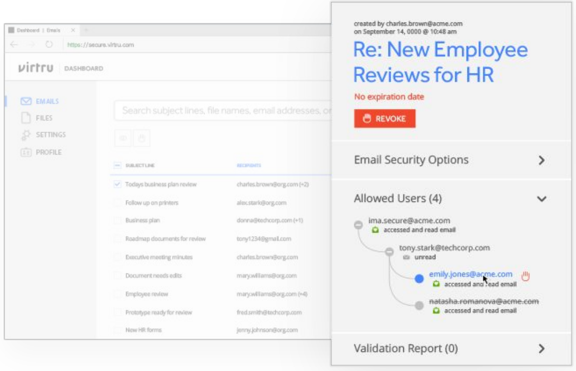
Thank you,

Officer Johnson

Secure_File_Attachment.pdf.tdf (83.9 kb)

- Disable Forwarding ✓
- Expires in: 2 days ✓
- PDF Watermarking ✓

Revoke or expire messages, control forwarding, view read receipt, and add watermarks to PDFs.



Dashboard | Emails

https://secure.virtru.com

virtru DASHBOARD

Search subject lines, file names, email addresses, or

SUBJECT LINE	RECIPIENTS
Todays business plan review	charles.brown@org.com (+2)
Follow up on printers	alex.stark@org.com
Business plan	donna@techcorp.com (+1)
Roadmap documents for review	tony1234@gmail.com
Executive meeting minutes	charles.brown@org.com
Document needs edits	mary.williams@org.com
Employee review	mary.williams@org.com (+4)
Prototype ready for review	fred.smith@techcorp.com
New HR forms	jenny.johnson@org.com

created by charles.brown@acme.com
on September 14, 0000 @ 10:48 am

Re: New Employee Reviews for HR

No expiration date

REVOKE

Email Security Options

Allowed Users (4)

- ima.secure@acme.com — accessed and read email
  - tony.stark@techcorp.com — unread
    - emily.jones@acme.com — accessed and read email
    - ~~natasha.romanova@acme.com~~ — accessed and read email

Validation Report (0)

Clear visibility into who has accessed or forwarded content.

virtru

“We didn’t really have a cohesive solution before Virtru. We had a few different legacy solutions that had been attempted over the years, but they were so cumbersome that no one really used them. Once we committed to Office 365, we started looking for something that would meet our security requirements, allow us to share with anyone inside or outside the company, and wouldn’t interfere with our users. That’s what put us on the path to Virtru.”

-Ken Kurz, Vice President of Information Technology and Chief Information Officer,
Corporate Office Properties Trust (COPT)

Modern Email Encryption

Functional Checklist

Modern Email Encryption Functional Checklist

User Experience

Recipient Access

- ❏ Seamless recipient workflow
- ❏ Uses existing accounts and applications to streamline collaboration
- ❏ No new usernames, or passwords

Customization

- ❏ Robust customization options
- ❏ Branded recipient experience to enhance trust and prevent confusion with phishing attacks

On-Demand Protection

- ❏ On-demand encryption available
- ❏ Clear end-user feedback within the user interface to improve security awareness
- ❏ No keywords or passphrases necessary to enable encryption

Security

End-to-End Encryption

- ❏ Encryption directly within the client
- ❏ Secure from sender to authorized recipient
- ❏ Protections prevent unauthorized access wherever sensitive data travels

Key Management

- ❏ Customer-hosted encryption keys that offer complete control and flexibility
- ❏ No potential for unauthorized government surveillance

Zero Trust

- ❏ Split-key architecture - encryption keys and content stored in separate environments
- ❏ Solution doesn’t require trusting vendor with access to unencrypted, sensitive content

Modern Email Encryption Functional Checklist

Audit and Access Control

DLP Controls

- ❏ Real-time, flexible controls available to both end users and admins
- ❏ Revocation, disable forwarding, expiration, PDF watermarking, and download and print restrictions
- ❏ Per-recipient, per-message granular controls

Auditability

- ❏ Complete audit trail with comprehensive accurate reports
- ❏ Clear visibility into when protected content has been read and where it has been forwarded

Internal Sharing Controls

Prevent Unauthorized Insider Access

- ❏ Strong, flexible internal controls
- ❏ Integrated DLP to detect and protect sensitive content shared internally
- ❏ Feature parity with external controls
- ❏ Consistent UX, whether sharing internally or externally

Administration

Configuration and DLP Rules

- ❏ Easy to set up and implementation
- ❏ DLP Rules can be configured and managed at group, OU, and individual levels, or across the entire enterprise
- ❏ Pre-defined rule templates available for common types of sensitive information

Ongoing Maintenance

- ❏ End-user DLP controls included to enhance security awareness and education
- ❏ User-assisted DLP decentralizes risk, reduces administrative overhead

Contact us for more information,
or to schedule a demo.

Start the Conversation

virtru

www.virtru.com