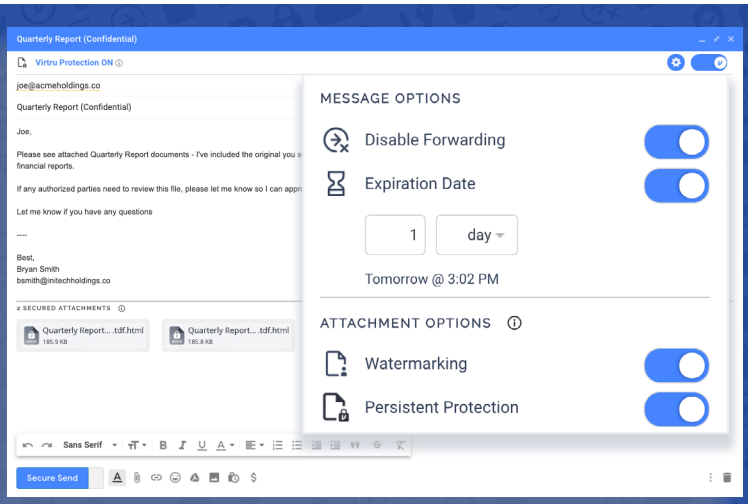
Virtru vs. Zix

Comparing Email Encryption Products



In today's fast-paced business world, email remains the most pervasive form of business communication. It's where companies create, store and share their most valuable information, so it's no surprise that it's also where unauthorized third parties look when trying to access corporate data.

When developing your secure email strategy, you must first understand that email platforms do have problems—breaches and hacks do occur and even the most modern email platforms (Google and Microsoft) aren't secure by default, so adding an additional layer of security with encryption is oftentimes mission-critical. Many customers require additional encryption and data protection capabilities to meet regulatory, compliance or privacy needs, such as:

- External sharing and control
- Object-level protection
- Data loss prevention (DLP)
- Cloud provider access levels
- Corporate governance
- Data residency
- Encryption key management
- Regulatory compliance (HIPAA, FERPA, CJIS, EAR, PCI, NIST, GDPR, CCPA etc.)

As organizations navigate the growing number of privacy regulations, security concerns in today's corporate ecosystems and the emerging complexities of the cloud, it's critical that they understand the additional encryption options available to them and how these solutions work.

Two of the most prominent email encryption solutions, Virtru and Zix, enable email and attachment file encryption for increased security and privacy, but they do so using very different approaches. What follows is a head-to-head comparison guide of Virtru's Email Encryption vs. Zix's flagship product, ZixEncrypt, evaluated in four key areas:

1. Sender Protections and UX
2. Recipient Access and UX
3. Administration
4. Security and Privacy

Capability of Offered Solution to Support Feature Need:

○ No solution ◔ Minimal solution ◑ Partial solution ◕ Good solution ● Complete solution

Sender Protections and UX

Feature	Virtru	Zix
Email Encryption	● End-to-end encryption for Gmail and Outlook.	◔ Only TLS-based encryption that cannot directly protect the data.
Attachment Encryption	◕	◔
Persistent Protection for File Attachments	● Protection beyond email to desktops, drives, etc. via HTML wrapper.	○
On-Demand, In-App Encryption and Controls	◕	○
Revoke Access / Recall Message	●	◔ Admin only.
Set Expiration	●	◔ Admin only.
Disable Forwarding	●	○
Attachment Watermarking	●	○
Read Receipt Visibility for Audit	●	○
Encrypted Search	●	○
Above Line Plaintext Intro to Improve Recipient Experience/ Access	●	○
Mobile Email Encryption App	◕	◔ Separate product (and cost).

Sender Protections and UX Summary:

The key point of differentiation is that Virtru offers end-to-end email encryption that's easy to use and supports both Gmail and Outlook. With Zix, the vast majority of deployments use ZixEncrypt, which doesn't support end-to-end encryption at all.

Virtru offers object-level email encryption and granular access controls, with persistent protections that allow protected sharing of attachments from email to desktops, content collaboration platforms (CCPs) and more. Zix's protections are TLS-based and don't enable control and visibility beyond email.

With easy to use controls, Virtru's senders can apply more granular and on-demand access controls (revocation, disable forwarding or expiration) within an intuitive UX. Zix senders are much more limited in that they cannot proactively apply controls, only admins can. Where Virtru offers watermarking support for common file types—including PDFs, Microsoft Office file types and images—Zix leaves sensitive attachments susceptible to leaks.

Once a message is sent, Virtru senders have clear visibility into who has accessed or forwarded every protected message. Zix senders can't view access and forwarding activity.

Recipient Access and UX

Feature	Virtru	Zix
Seamless Authentication	●	◑
Branded Recipient Email Template	● Custom text, logos and graphics.	◔ Custom text only.
Branded Read / Consumption Experience	●	◕
Recipient Send / Reply Encrypted Support	◑	◑
Additional Recipients / Collaborator Support	●	○
Mobile Access	●	◑

Recipient Access and UX Summary:

Virtru offers modern, seamless recipient access and secure collaboration workflows that support dynamic sharing using Secure Reader, while Zix's support for external recipients is limited, with extra steps to access the email and limitations on additional collaborators.

Virtru pioneered the use of federated identities to enable seamless, secure access for recipients. Zix has also developed a recipient access workflow via federated identity that removes the need to create a Zix portal account and password, but this feature may not be available in all deployments or access workflows.

Zix provides basic customization of recipient email and the Zix Portal with text and logos, but Virtru provides more robust graphics support to fully customize the recipient email and Secure Reader experience with the customer's branding.

Administration

Feature	Virtru	Zix
Administration Console	Centralized admin console via Virtru Control Center.	Different consoles for audit, DLP and user management.
Users Administration		Permissions management is separate from user activity logs.
Revocation / Recall on Behalf of Senders	Per message, sender or recipient OR mass revocation via filtering.	Per-message only.
Change Expiration Date on Behalf of Senders		Message expiration must be changed in separate app from expiration policies.
Disable Forwarding on Behalf of Senders	Per-message disable forwarding.	Disable forwarding via policy only, not per-message.
Read / Access Visibility		

Administration cont.

Feature	Virtru	Zix
Audit Reporting and Event Logs	◑ Log export support.	◕ Dashboard with canned summary reports and visualizations with log export support.
SIEM Integration	●	●
Data Loss Prevention	◑ Integrated DLP with preconfigured rules and ability to create custom rules.	◕ Enterprise DLP via Digital Guardian partnership.

Administration Summary:

The main point of differentiation for administration is ease of use. Virtru's administration capabilities are available via the Virtru Dashboard as a single, centralized administration portal. With Zix, administration is spread across several separate applications.

Virtru offers administrators powerful and intuitive ways to revoke access, change expiration and disable forwarding, at scale or at a granular per-message level to keep data protected as its context evolves. Zix's administrators can't disable forwarding at the message level and changing an expiration date forces admins to use a separate application than where they originally set the expiration policy.

Virtru and Zix both log system events and make that event data available for audit reporting and SIEM integrations. Zix offers a dashboard with canned reports and visualizations.

Both Zix and Virtru offer integrated DLP with a broad set of pre-configured rules. Zix's partnership with Digital Guardian for enterprise DLP offers even more robust DLP rule templates, though this is sold—and managed—separately.

"With Virtru, we are not adding any additional layers of complexity to our email workflows. Everyone—from the CEO to our case managers—agrees that Virtru doesn't obstruct the way we communicate over email, but rather makes for a better experience."

- Shaun Michel, IT Director at Valley Youth House

Security and Privacy

Feature	Virtru	Zix
No Third-Party Access to Plaintext	●	○
Customer-Hosted Keys	●	○
HSM Integration	◕	○
FERPA Compliant	●	●
HIPAA Compliant	●	●
CJIS Compliant	◕	○

Security and Privacy Summary:

Most Virtru deployments leverage client-side, end-to-end encryption for Gmail and Outlook, preventing third-party access to keep email private. Most Zix deployments use ZixEncrypt, which gives Zix and the underlying cloud provider access to the data.

For enhanced security, Virtru Customer Key Server gives customers the option to host and manage the encryption keys protecting their data for absolute control, with HSM integration support. Zix doesn't offer any customer-hosted key or HSM integrations.

Virtru customers can fulfill compliance requirements for CJIS to keep criminal justice data private with end-to-end encryption, whereas ZixEncrypt doesn't support CJIS compliance as it is not end-to-end encrypted.

"With Zix, we were never able to actually see if an email was secure—much less be able to revoke something sent in error. With Virtru, we have very hands-on, flexible administration that gives us more control. If we need to revoke an email, we can. If we need to track an email to ensure it was encrypted, we have that ability."

- Ben Baez, Application Administrator, Bancroft

Conclusion

In a modern world where innovation is driven by collaboration, organizations must ensure not only that their email encryption solution doesn't slow them down, but that it protects their most sensitive data at all times.

Zix's portal-based encryption doesn't meet modern needs. Where it fails, Virtru succeeds with ease of use and end-to-end protection that provides unmatched visibility and control. Virtru's end-to-end encryption and persistent access controls better support protected sharing workflows to give senders and admins greater assurances that email stays private, wherever it's created or shared.

Where Zix falls short, Virtru provides:

- A reliably seamless, secure user experience with more granular controls.
- Centralized administrative experience.
- The option for organizations to host their own keys and integrate with HSMs for the highest levels of security and control.

The best way to secure your data is with data-centric protection. Data-centric security focuses on protecting the data itself regardless of where it is hosted, from applications to the body of an email.

To truly eliminate risks and develop a strategy for complete email protection, reinforce native Gmail and Microsoft encryption with a third-party solution that provides strong, data-centric encryption. This ensures that unauthorized users—such as hackers, your email provider or even your third-party encryption provider—are not able to access your content.

Virtru's end-to-end encryption ensures that all data is encrypted at all times—not just in transit and at rest—and that only the sender and recipient can view the contents of an email, providing the highest level of confidentiality and protection to your organization's emails.

Learn how you can easily protect data wherever it's created or shared.
Contact us today at **virtru.com/contact-us**.