



Mitigate Risks and Gain Control of Your Data

Why You Should Add Virtru Data-Centric Encryption to Microsoft 365

In this Guide

- Introduction: A Data Protection Solution That’s Built for You 2
- Solve Challenges to Make Data Sharing Secure Yet Simple 3
- Review Virtru and Microsoft Encryption Architectures..... 4
- Compare Virtru to Microsoft E3 and E5 Plans 5
- Conclusion: It’s Your Data and Virtru Helps Keep it That Way10

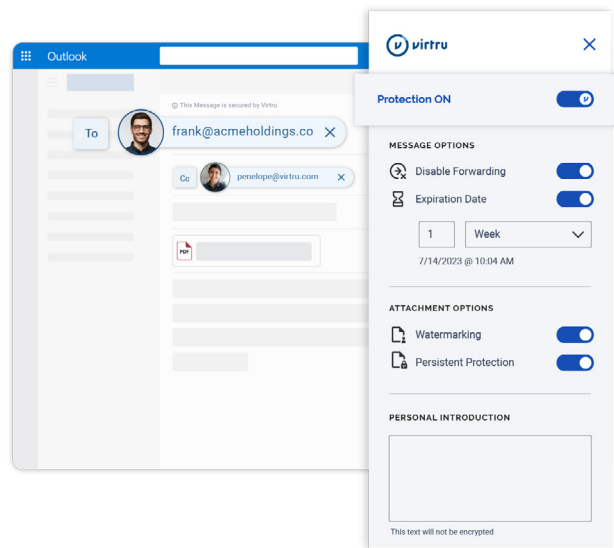
Introduction: A Data Protection Solution That's Built for You

Protection for data sharing across digital workflows requires trusted data encryption and specific access control capabilities as privacy needs can change at any moment. When it comes to Outlook, there are numerous providers, including Microsoft's Enterprise plans, to choose from. The key is finding a solution that delivers the most value, from security requirements to functionality to ease of use, for your organization.

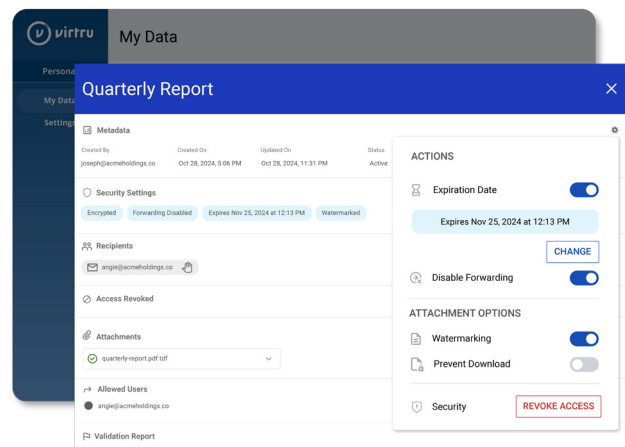
The right solution will help you maintain control and visibility of your data throughout its lifecycle, preserve privacy, and mitigate risk. That's achieved by delivering on everything from a Zero Trust architecture, flexible encryption key management, cloud interoperability and integration options, and user-friendly access controls.

Create an end-to-end data protection solution with Virtru to quickly deploy and easily manage security organization-wide, improve collaboration, control access to your data, and enable business alignment. Get exactly what you need and only pay for what you'll use. Virtru products for Microsoft include:

- Outlook Add-in: Apply Virtru data-centric encryption and granular access controls directly within Outlook, and wrap each data object in its own layer of encryption, so you can manage data anywhere it travels.
- Virtru Private Keystore: Host your private encryption keys anywhere and collaborate with total confidence that your data remains under your control.
- Data Protection Gateway: Secure outbound emails sent by apps such as Salesforce and Zendesk, and use inbound encryption for responses from Workday or HR tools so you are protecting data when and where it's needed.



Turn on Security Rules for text patterns in messages



Review data access and forwarding activity, and adjust access controls

Solve Challenges to Make Data Sharing Secure Yet Simple

Our mission is to help you unlock the power of your data by maintaining control everywhere your data travels and is shared. With that in mind, Virtru's solutions help solve your biggest data sharing challenges.



Meet the highest security requirements

Virtru helps you meet compliance requirements including CJIS, ITAR, CMMC, GDPR, and HIPAA without an exorbitant price tag, while being easy to use to prevent human error. We are a seamless part of your overall compliance solution.



Prevent third-party access (including cloud and email providers)

Virtru offers options for encryption key management to support regulatory compliance, data sovereignty, and data residency including the ability to host your own keys so you have an additional layer of security wherever your data is created or shared. This means you can prevent any third-party (including Virtru and Microsoft, as well as other cloud, email, and security vendors) from accessing your data.



Easily add the right level of access control to any message

Virtru offers granular access controls (including revocation, forwarding control, expiration date, watermarking, and persistent file protection) for each user/sender as well as advanced controls for admins to manage data organization-wide. These are available to all of our customers—not excluded by price or package, and not limited to just external recipients, as internal emails also need data management and control.



Extend encryption and access control to attachments

Virtru delivers flexible and comprehensive access controls for file attachment including Microsoft Office files, PDFs, image files, etc. These controls include watermarking to prevent downloading or printing, as well as persistent file protection so you maintain control and can revoke access, no matter where that file is saved.



Collaborate across ecosystems and platforms, and never worry about recipients using different email clients or levels of network security

Virtru works seamlessly across ecosystems, without losing data security, residency, or control, no matter what email client or security setup the recipient has in place. Virtru also supports both Google and Microsoft in hybrid environments, so you can maximize agility and adapt to new requirements without being locked into one email client.



Use a solution that is easy to manage and decreases total cost of ownership

Virtru offers quick implementation and adoptability, so you'll see fast value. Admins can easily deploy and manage data organization-wide. Users are empowered to protect data because it is easy to add encryption and important access controls. Completing the data lifecycle, recipients have ease of access without requiring new accounts or passwords. Avoid the headache of trying to navigate numerous solution pages, conflicting documentation, and overlapping but uninteroperable solutions from Microsoft.

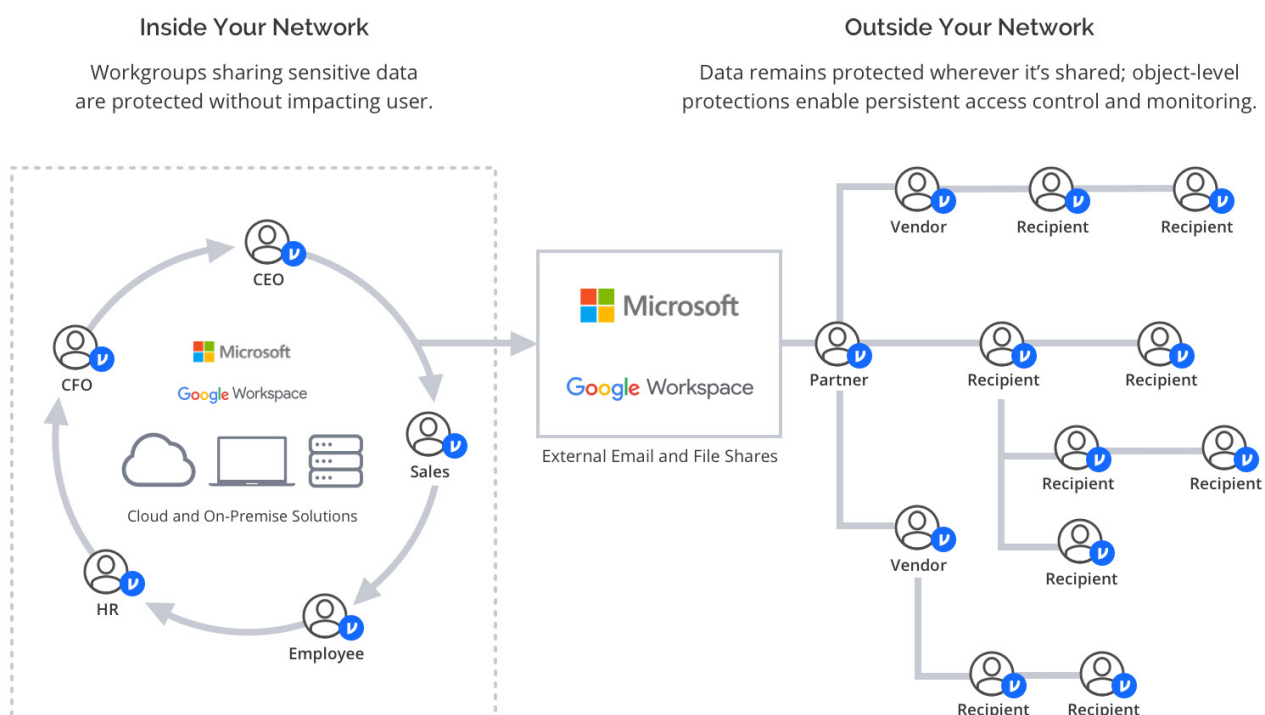
Review Virtru and Microsoft Encryption Architectures

The foundation of Microsoft’s data protection for email is Microsoft Purview Message Encryption, which is an online service that’s built on Microsoft Azure Rights Management (Azure RMS) and part of Azure Information Protection. This service includes encryption, identity and authorization policies to help secure email. Azure RMS’s persistent protection helps secure the data because protection settings remain with that data.

Microsoft bundles this encryption with other data security features for enterprise and mid-market organizations into Enterprise plans. Most notably their E3 and E5 plans look to improve data collaboration by enhancing encryption with access controls, DLP rules, and data reporting/intelligence to meet regulatory compliance and secure data from unauthorized access.

The foundation of Virtru lies in the Virtru Data Security Platform, which stores encrypted content apart from the encryption keys, supporting a Zero Trust framework where all system components are continuously authenticated. Virtru is powered by the open-sourced, Virtru Trusted Data Format (TDF) that keeps data protected and under the owner’s control no matter where that data travels or where it’s saved. With the TDF, an organization can apply discrete policies and rules leveraging Attribute-Based Access Control (ABAC) that travel with the content.


For your focus on data protection and compliance, Virtru adds incremental value to securely collaborate with ease. To meet data security, we offer encryption key management options including hosting your own encryption keys, seamless platform integration options, and cloud interoperability. For optimal functionality, we offer granular access controls to manage data shared internally or externally. And, we offer flexibility to create a package of services to meet your exact requirements with patented ease of use for admins, users, and recipients to enhance any data sharing workflow.
















Compare Virtru to Microsoft E3 and E5 Plans













There are some key areas where Microsoft E3 and E5 do not deliver the same data protection value that Virtru can for your organization—particularly for highly regulated industries. While Microsoft’s high-priced, government-tier plans can meet these rigorous data protection standards, Virtru offers the same level of comprehensive data protection to every customer. The following chart reviews the capabilities of Microsoft E3 and E5 when compared to Virtru so you can better understand how each data protection solution aligns with your needs.

Capabilities		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Encryption & Data Governance	Send Encrypted and Rights-Protected Messages	 Data-Centric, End-to-End Encryption	 Office Message Encryption	 Advanced Message Encryption
	Encrypt/Protect Messages at the Object Level to Control Access at Any Time	 Access Message	 Ensure Azure Information Protection (AIP) is being used  Legacy versions of Office Message Encryption	 Ensure Azure Information Protection (AIP) is being used  Legacy versions of Office Message Encryption
	Support a Zero Trust Security Model Across Browser, Desktop, and Mobile Outlook Experiences	 Support for every way you use Outlook today		 Double Key Encryption in this package only supports the desktop version of Outlook on Windows (not in web browsers or on a Mac/ iPad)
	Ensure Plain Text Cannot Be Accessed by Any Third Party	 Virtru (and other providers, including Microsoft) cannot access your content under any circumstance—we just manage access policies and broker key exchanges		 Customer Lockbox- Microsoft cannot access your content without your explicit approval, but this shows they can still access your content in some way

Capabilities		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Encryption & Data Governance	Customize DLP Rules	 Set rules and actions for text patterns, keywords, and recipients; use our pre-built rule pack for HIPAA; or create your own custom rules		 Offers more advanced condition and action setting, and generates incident reports
	Detect and Investigate Advanced Threats	 Offers ability to investigate outlier activity and unauthorized access		 Microsoft Defender Advanced Threat Protection (ATP)—pre-breach prevention and post-breach investigation for sophisticated attacks such as phishing and malware
	View Actionable Data Intelligence	 Virtru Control Center allows admins to see what data their organization is protecting, know where it's going, manage who it's shared with, and ensure it stays under the appropriate control		 Admins have visibility into activities related to sensitive data sharing, including where sensitive data is stored, encryption activities, and data loss prevention (DLP) logs
	Inbound Email Encryption			

Capabilities		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Support to Help Meet Regulatory Compliance	HIPAA	✓	✓	✓
	GDPR	✓	✗	 <p>Double Key Encryption is best practice, but this is limited to Outlook on Windows</p>
	CJIS	✓	✗	 <p>Requires highest-priced Government Service Plans (GCC for state and local government and GCC High for federal)</p>
	CMMC	✓	✗	 <p>Requires highest-priced Government Service Plans</p>
	ITAR	✓	✗	 <p>Requires highest-priced Government Service Plans</p>

Capabilities		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Interoperability	Operate with Any Public Cloud Provider			
	Support a Hybrid Use Model (Both Google and Microsoft)			
	Recipients With Any Email Client or Security Setup			PARTIAL Depends on deployment model; some options do not allow for external delivery of email OR require existing software for recipients
	Ensure Plain Text Cannot Be Accessed by Any Third Party	 Virtru works no matter what email client or security setup the recipient has in place and Virtru can never access your data	 If your email travels outside of the Microsoft ecosystem, you might lose data security, residency, and control, and Microsoft can access your data	PARTIAL Depends on deployment model; greater privacy may result in usability & sharing restrictions

Capabilities		Virtru	Microsoft 365 E3 Plan	Microsoft 365 E5 Plan
Access Control Flexibility and Adaptability	On-Demand Access Controls Available to Both Admins and Users/Senders	 Out-of-the- box, granular access controls for message	 Limited access controls—only offers “do not forward”	 However, access controls require admin configuration
	Easily Add and Adjust Expiration Dates for Internal or External Recipients	 Support for every way you use Outlook today	 Not Offered	 Only admins can change expiration policies, and expiration is limited to external recipients
	Easily Revoke Emails Sent to Internal or External Recipients	 Support for every way you use Outlook today	 Not Offered	 Revocation is limited to external recipients
	Access Controls and Protection Extend to File Attachments	 Watermarking and persistent file protection for most file formats to maintain control and revoke access at any time	 Microsoft Office attachments such as Word remain encrypted, but other formats such as PDFs can be downloaded without protection	 Microsoft Office attachments such as Word remain encrypted, but other formats such as PDFs can be downloaded without protection

Conclusion: It's Your Data and Virtru Helps Keep it That Way

Virtru is a seamless layer of data protection on top of your native Microsoft experience, so your team can easily protect messages and attachments and maintain control everywhere they're shared. Whether using Outlook from a browser, desktop, or mobile device, on your PC, Mac, iPad, or phone, Virtru helps keep your data secure.

To support your needs, Virtru delivers:

- Data-centric protection and Zero Trust data governance to securely collaborate with authorized recipients and ensure no third party can access your data.
- Encryption key management options to meet compliance and data sovereignty.
- Protection to secure messages sent and received by custom or enterprise SaaS apps.
- Support for a hybrid use model where both Microsoft and Google are deployed.
- Access controls, including instant revocation, message forwarding control, expiration date, file watermarking, and persistent protection of downloaded attachments, so everyone can protect data shared internally and externally.
- Ease of use to deploy and manage data security, including customizable email rules.
- Quick user adoption to prevent human error when sending sensitive information.
- Actionable intelligence across data to clearly see what data you're protecting, where it's going, and who has read or forwarded it.
- Seamless recipient access without requiring new accounts or passwords.

“The financial industry is particularly susceptible to attack because of the prevalence of sensitive data, but with Virtru's unmatched ease of use, we are assured that our clients' and partners' most sensitive data is protected.”

-Security Director, Financial Services Business

More Than 7,000 Customers Trust Virtru for Data Security and Privacy Protection.



See how Virtru can enable privacy and compliance for Microsoft 365 Outlook: virtru.com