

Virtru + Google vs. Microsoft

Moving from Microsoft to Google with the Combined Benefit of Virtru Zero Trust Data Access



Data protection initiatives are focused on eliminating security gaps in the data lifecycle as you create, share, use, and store data. Google Workspace combined with Virtru’s Zero Trust Data Access platform gives you and your people a simple way to share data without sacrificing security, privacy, or control – all while complying with important data privacy regulations. Virtru and Google deliver on the needs of Zero Trust data protection as well as the differentiators of: ease of use for admins/users/recipients, simple deployment, and fast user adoption to see security results across your internal organization and collaboration network.

Comparing Capabilities and Benefits: Virtru + Google vs. Microsoft

	Virtru + Google	Microsoft
Encryption, Data Access, & Data Governance	Use end-to-end encryption that protects emails and files at the object level to control access at any time	<ul style="list-style-type: none"> ✔ Only supported if using Azure Information Protection (AIP) ✘ Not supported for legacy versions of Office Message Encryption
	Support a Zero Trust security model across browser, desktop, and mobile experiences	✘ Requires Microsoft Double Key Encryption, which is only supported on desktop version of Outlook on Windows machine*
	Ensure plain text cannot be accessed by any third party (including Virtru and Google) at any time	<ul style="list-style-type: none"> ✘ This depends on the specific Microsoft plan you use <p>In E1 and E3 plans, Microsoft can access your plain text. In higher priced E5 plan, Microsoft won't access your content without your explicit approval, but this shows they can still access plain text in some way</p>
	Securely email recipients with any email client or security setup	✘ If your email travels outside of Microsoft ecosystem, you might lose data security, residency, and control

*Additional limitations of Microsoft Double Key Encryption: Many features inside Microsoft 365 will not function such as SharePoint Search, eDiscovery Search, DLP, Transport Rules, Exchange ActiveSync, Journaling, Malware Scanning, and Archiving Solutions

	Virtru + Google	Microsoft
Encryption, Data Access, & Data Governance	View actionable data intelligence	 Most Microsoft plans only offer an index of sensitive documents stored within supported Microsoft 365 workloads
	Encrypt inbound emails	 Not supported
Support to Help Meet Regulatory Compliance	HIPAA	
	GDPR	 Microsoft Double Key Encryption is best practice, but this is limited to Outlook on Windows
	CJIS, CMMC, ITAR & EAR	 Requires highest-priced Government Service Plans (GCC for state and local government and GCC High for federal)
Access Control Flexibility and Adaptability	Have on-demand access controls available to both admins and users	 Limited access controls—many plans only offer “do not forward” and higher priced plans require admin configuration
	Easily add and adjust expiration dates for internal or external recipients	 Only admins can change expiration policies, and expiration is limited to external recipients
	Easily revoke emails sent to internal or external recipients	 Revocation is limited to external recipients
	Extend access controls and protection to file attachments	 Microsoft Office attachments such as Word remain encrypted, but other formats such as PDFs can be downloaded without protection

Zero Trust Data Access Built to Share, Control, and Protect Your Data

Adding the Virtru Zero Trust Data Access platform to your Google migration gives you the power to control your data no matter what providers, platforms, or SaaS solutions you use, the ease of use to create simple, efficient workflows, and the freedom to share data any way you need to. Secure the data itself for protection everywhere.



Learn how you can protect your data with Virtru.