Kiteworks

PRODUCT BRIEF

Choosing Kiteworks Over Microsoft Purview Means Choosing Best-of-Breed Protection

For sending and receiving highly sensitive information, Microsoft Purview protection just isn't good enough.

Multitenant Is Vulnerable

Imagine if your sensitive content and encryption keys co-mingled with hundreds of other companies' content and encryption keys in a single server. Would you consider that a secure environment? Neither would we, but that's how Microsoft achieves scale and cost efficiencies in its Microsoft 365 customer base. The dark side of multitenancy is that an attacker can use a single vulnerability to gain access to an entire environment, thereby cross-breaching into multiple customers' datasets with one attack, as was the case with the August 2020 Azure Cosmos DB vulnerability.[1] Kiteworks Enterprise is always single tenant. Your data is air gapped from other customers because it does not share an environment, ensuring another's weakness is not an exploitation into your data.

Encryption Is Leaky

Microsoft Office 365 Message Encryption (OME) uses a weak cryptographic algorithm, Electronic Codebook (ECB), which attackers can exploit to obtain sensitive information from emails.[2] Researchers at WithSecure showed how information leaked by individual emails can be combined, such as in the case of a breached email server or backup, to infer sensitive content. Kiteworks safeguards emails and attachments with strong encryption exclusively, including AES-256, TLS, S/MIME, and OpenPGP, depending on the components and options used.

The Default Access Settings Are Insecure

Bucking the trend of zero trust, where the default is least-privilege access, anonymous sharing is enabled by default for SharePoint and OneDrive in Microsoft 365. This enables end-users to share files and folders from within OneDrive without requiring the recipient to sign in or use a password to access the file. Anyone receiving the link can also access the shared file, so there is no restriction on the original recipient forwarding the link to multiple people and unintended recipients.[3] Kiteworks, on the other hand, uses least-privilege defaults for all settings. Users must be granted explicit access to content, and explicit rights to forward it, by admins or trusted business managers. Admins control which user profiles are trusted to share or send content, as well as those users' default and maximum privileges for forwarding, expiration, digital fingerprinting, and other policies. To prevent accidental exposure of sensitive content, an administrator who changes a policy to a potentially risky setting receives a detailed warning of the risk and needs to confirm their choice.

Microsoft Has Visibility Into Your Data

When using Microsoft-managed keys or BYOK, Microsoft can be issued a subpoena or warrant by a government to turn over your data, and they don't have to alert you when they comply. The only solution for fully blind-to-Microsoft keys is Microsoft's Double Key Encryption;[4] it requires additional key management overhead and resources, and most important, disables your ability to apply security transport rules such as anti-malware.

Because of this, Microsoft recommends using it only for your "most sensitive data," equating to 1-2% on average. With Kiteworks, all 100% of your sensitive content is safe from our eyes out-of-the-box.

Email Encryption Complexity Drives Shadow IT

Using Microsoft OME encryption can cause productivity issues when recipients try to access information. OME requires acquisition of a one-time passcode from the sender or requires the recipient to sign in with a Microsoft account. For those who use Gmail or other email systems, frustration with this gating can lead senders and recipients to make "side deals" that bypass security to get their jobs done.[5] Kiteworks emails are encrypted and decrypted seamlessly, and recipients use their native email accounts. It provides a range of email encryption architecture options, such as web and mobile clients, Outlook integration, and end-to-end encryption using standard email clients without plugins.

Large Files Create Bottlenecks and Insecure Behavior

With Microsoft, file size limitations such as 20 MB[6] in emails and 250 GB[7] in OneDrive and SharePoint force users to search for an alternative solution when sharing sensitive information beyond these limits. More often than not, this alternative transport is insecure and unauditable. With Kiteworks, customers are provided virtually limitless, reliable file transfers up to 16 Terabytes, which allows heavy sensitive files such as videos or IP in the form of CAD/CAM drawings or DNA sequences to be shared without worry.

Geofencing Gap

Neither OneDrive for Business nor MDM for Office 365 can enforce usage rules based on location.[8] This means Microsoft customers can't protect your data from access by potential malicious actors in known suspect nation-states, nor is it straightforward for Microsoft customers to isolate data access and sharing based on data sovereignty regulations. Kiteworks, on the other hand, enables administrators to block access from within specific countries or IP address ranges for all users or for specific user profiles/roles. While both Microsoft and Kiteworks policy settings can force specific users' data to be stored in their home countries, Kiteworks customers can enforce sovereignty to the strictest level—an air gap between countries—by deploying separate Kiteworks instances in separate countries, such as Germany and China.

[1] Joseph Menn, "EXCLUSIVE Microsoft warns thousands of cloud customers of exposed databases," Reuters, August 27, 2021.

[2] Nathan Eddy, "Microsoft 365 Message Encryption Can Leak Sensitive Info," Dark Reading, October 14, 2022, and "Weakness in Microsoft Office 365 Message Encryption could expose email contents," Help Net Security, October 14, 2022.

[3] Chris Jackson, "The Top 10 'Gotchas' of SharePoint in Microsoft 365," Gartner, November 3, 2022.

[4] K.C. Cross, David Strome, et al., "Double Key Encryption," Microsoft, November 15, 2022.

[5] K.C. Cross, David Strome, et al., "Email encryption," Microsoft, October 18, 2022.

[6] "Send large files with Outlook," Microsoft Support, 2022.

[7] "Upload photos and files to OneDrive," Microsoft Support, 2022.

[8] "Content Collaboration Platform In-Depth Assessment Comparison," Gartner Cloud Decisions, September 11, 2019.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.

www.kiteworks.com

November 2022