Top 5 Reasons Kiteworks Email Encryption Outperforms Microsoft 365

Stronger Algorithms, Safer User Behavior, Safer Cloud

Kiteworks encryption outperforms Microsoft's algorithms. Just as important, it strengthens protection against user behavior and cloud threats that can make even the best encryption algorithms irrelevant.

Microsoft OME .RPMSG File Uses a Leaky Encryption Algorithm

Attackers can exploit cryptographic weaknesses of RPMSG encryption to obtain sensitive information from email attachments, according to researchers at WithSecure Labs. "Outlook 365 Message Encryption [OME] uses Electronic Codebook (ECB) mode of operation when encrypting the message into RPMSG blob ... This mode is generally insecure and can leak information about the structure of the messages sent, which can lead to partial or full message disclosure." Kiteworks safeguards emails and attachments with strong encryption exclusively, including AES-256, TLS, S/MIME, and OpenPGP, depending on the components and options used.

Large Files and External Users Can Drive Insecure Behavior

This may seem obvious, but your email encryption product only works when employees actually adopt it in their communication with external business partners, customers, attorneys, and regulators. And when users have trouble getting that job done, typically due to file size limits or a difficult user experience, they may look for alternative methods. When that happens, the organization may lose both security and auditability of file transfers.

With Microsoft, file size limitations are as low as 20 MB in emails, including encrypted .RPMSG attachments, and 250 GB in OneDrive and SharePoint. This incents users to work around the system when they send large analytics datasets, video evidence, DNA sequences, CAD files, and other sensitive information. Kiteworks email seamlessly transfers encrypted files as large as 16 TB to make sure employees never have a reason to bypass the secure, compliant method you've provided.

Next, picture an employee who sends a Microsoft Office 365 email to recipients whose email system isn't Microsoft Office 365 or a federated partner. Those recipients have two ways they can receive and decrypt it: create and use a Microsoft account instead of their organization's email system, or request a one-time password for each email they need to open. Kiteworks research shows employees and their external partners may use alternatives like consumer file sharing to work around such difficulties. Kiteworks, on the other hand, always makes it easy for external recipients to open encrypted messages in their native environment, thus ensuring security and auditability.

Kiteworks Simplifies S/MIME and OpenPGP Usage to Avoid Shadow IT

Your organization may have partners who require communication via S/MIME or OpenPGP encryption. Microsoft's S/MIME product puts users through the frustration of understanding and handling public and private keys. This gives them an incentive to find an unsanctioned alternative that may expose your organization to the risks of security breaches, leaks, and compliance fines. Microsoft does not support OpenPGP.

The Kiteworks Email Protection Gateway (EPG) provides a simple S/MIME and OpenPGP experience, so users don't have to change the way they work. It makes key exchange invisible to end-users, and it works with the standard email clients employees and external parties already use. EPG even automates key administration.

A Kiteworks EPG user can send a single encrypted email to any combination of S/MIME and OpenPGP recipients to provide the ultimate in simple flexibility. Kiteworks EPG also provides unique end-to-end encryption that enables scans such as antivirus, DLP, and advanced threat prevention (ATP), yet makes decryption impossible for unintended external listeners as it crosses the internet.

Avoid Multitenant Vulnerabilities With Kiteworks Private Cloud

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. 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.

Microsoft Has Visibility Into Your Cloud 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; 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.