Kiteworks

Top 5 Ways Kiteworks® Secures Microsoft 365 Third-party Communications

Many IT security teams are now re-evaluating their Microsoft 365 cloud and Microsoft on-premises software stack after the recent attacks against Exchange. They often find its cloud and on-premises protection inconsistent, and it raises additional auditing and data control challenges for third-party communications. Many Microsoft 365 controls were not designed to secure third-party communications, but with the escalating volume of attacks, those communications require specialized layers of defense.

The Kiteworks® Private Content Network (PCN) provides five essential protection layers around Microsoft 365 offerings such as E3, E5, and GCC. Kiteworks paired with E3 is often considered more cost-effective and secure than E5 and GCC alone.

1. Immutable and Comprehensive Microsoft 365 Auditing

IT security teams managing a breach or executing an audit often discover that their Microsoft 365 log data is either 1) delayed, 2) missing, or 3) unconsumable. Kiteworks provides real-time centralized auditing and alerting of third-party file transfers to and from Microsoft 365, Outlook, SharePoint, Teams, and OneDrive. While Microsoft 365 often throttles its logging during periods of high activity —like breaches—the comprehensive Kiteworks log ensures every entry is captured, indexed, and unified across all connected products. Kiteworks stores its immutable audit logs in hardened environments away from Microsoft 365 storage for even more protection.

2. Secure and Compliant OneDrive Sharing

End-users save their most sensitive documents in OneDrive, and they can reveal them to the world if external sharing is not disabled. Administrators can't accurately govern who has access to which OneDrive content when third parties authenticate indirectly, using other Microsoft account credentials instead of Microsoft 365. Kiteworks can put a layer of protection around OneDrive content and safely share it with third parties. IT security teams can maintain full OneDrive control and demonstrate compliance with comprehensive logging and reporting.

3. Secure and Unlimited Sized File Sharing

End-users often take risky approaches when sending large content to third parties because Outlook has a fairly small file size limit. They either try to share it unsafely on Onedrive or revert to other insecure forms of communication. Kiteworks allows users to send unlimited size files securely and easily to third parties within Outlook via the Kiteworks plugin.

4. Zero Trust Phish-proof Email

End-users fall victim to phishing emails despite Microsoft email filters. The reason is simple: Microsoft Outlook accepts emails from any email address. Kiteworks Secure Email only accepts emails from authorized addresses, thus disallowing virtually all malicious sources.

5. Private Deployment for Complete Data Control

Sensitive data stored in Microsoft 365 can be used and/or subpoenaed without your approval because your encryption keys reside in Microsoft's public cloud environment. Control access by holding your own key (HYOK) in your environment via Kiteworks' private cloud, FedRAMP private cloud, and on-premises deployment options. Even regulations such as the U.S. Federal CLOUD Act cannot force Kiteworks to release your data.