Kiteworks

Top 5 Ways Kiteworks Platform Secures Third-party Box, OneDrive, and Teams Communications for Government Agencies

Suppliers, vendors, consultants, and contractors deliver tremendous value to federal and central government agencies but also add tremendous risk. While agencies may repel direct cyberattacks, network defenses cannot prevent hackers from island hopping in when IP, PII, and PHI are exchanged with third parties. Box, Microsoft OneDrive, and Teams are a popular combination set of file sharing and collaboration tools for government agencies, but their popularity also attracts hackers. Both Box and Microsoft offer security controls to combat the onslaught of attacks, but these security controls were not designed to secure third-party communications. The following are five Kiteworks platform capabilities that help address third-party communication risk when using Box, OneDrive, and Teams.

1. Uniform Security and Governance for Cloud Services

Government agencies use various cloud services, and security and governance across all these cloud services are essential, but OneDrive only covers its own service, and Box only integrates with Microsoft 365 and Google Drive. The Kiteworks platform protects all content entering and leaving the organization across all communication channels, including content shared from popular cloud services like OneDrive, SharePoint, Box, Dropbox, and Google Drive. Kiteworks wraps these services in a uniform layer of security and governance. Plus, detailed audit logs provide complete traceability, so you know who has your IP regardless of how it was shared, and you can protect the IP, PII, and PHI shared with you.

2. Secure and Unlimited Sized File Sharing

End-users often revert to other insecure forms of communication when sending large content to third parties because Box has a small file size limit of 32 GB and OneDrive with 250 GB. Kiteworks allows users to send unlimited size files securely and easily to third parties. For even better workflow, users can even send large files from popular mail clients such as Outlook via the Kiteworks plugin.

3. Private Deployment for Complete Data Control

Sensitive data stored in Box and OneDrive can be used and/or subpoenaed without your approval because your encryption keys reside in Box and OneDrive'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.

4. 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.

5. Secure and Compliant Teams Sharing

End-users collaborate with external parties over Teams, but Teams cannot transfer files to external or guest users. The Kiteworks Teams plugin allows users to securely share proposals, budgets, presentations, and other sensitive documents with guests and external users directly within Teams.