Top 5 Ways the Kiteworks® Platform Secures Box®, OneDrive® and Teams® 3rd Party Communications for Government Agencies

KITEWORKS CONTENT FIREWALL

Suppliers, vendors, consultants, and contractors deliver tremendous value to federal and central government agencies but also add tremendous risk. While agencies may repel direct cyber-attacks, network defenses cannot prevent hackers from island hopping in when IP, PII, and PHI are exchanged with 3rd parties. Box, Microsoft OneDrive, and Teams constitute a popular 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 controls were not designed to secure 3rd party communications. The following are five Kiteworks content firewall capabilities that help address 3rd 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. However, OneDrive only covers its own service, and Box only integrates with Microsoft 365 and Google Drive. The Kiteworks content firewall 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. It 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 3rd parties because Box has a small file size limit of 32 GB and OneDrive has a limit of 250 GB. The Kiteworks platform allows users to send files of unlimited size securely and easily to 3rd parties. Users can even send large files from popular mail clients such as Outlook via the Kiteworks plug-in for better workflow.

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. You can control access by holding your own key (HYOK) in your environment via Kiteworks private cloud, FedRAMP private cloud, and on-premises deployment options. Therefore, even regulations such as the U.S. Federal CLOUD Act have no way to force the data to be released.

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 3rd parties authenticate indirectly using Microsoft Account credentials other than Microsoft 365. The Kiteworks content firewall can put a layer of protection around OneDrive content and safely share it with 3rd parties. IT security teams can maintain full OneDrive control and demonstrate compliance with comprehensive logging and reporting.

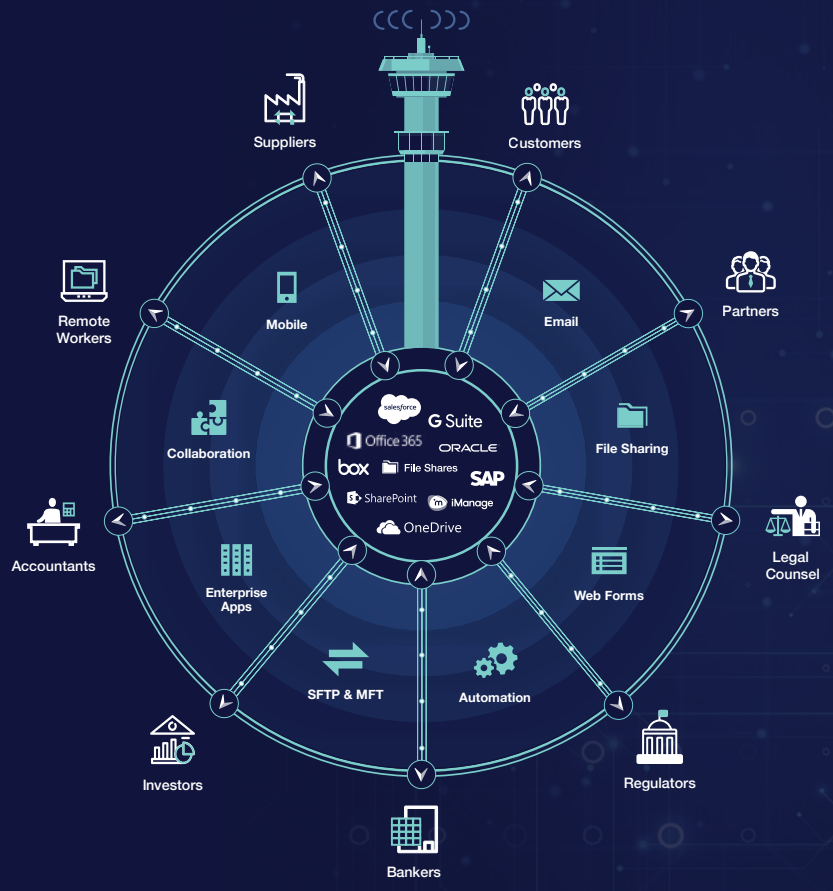
5 Secure and Compliant Teams Sharing

End users collaborate with external parties over Teams, but Teams cannot transfer files to external or guest users. The Kiteworks Teams plug-in makes it easy, secure, and compliant for users to share files with guests and external users directly within Teams, protecting sensitive documents like proposals, budgets, and medical images. They can even send files well over a terabyte, like massive software logs and bodycam evidence videos.

Kiteworks Content Firewall: Going Beyond Box and Microsoft

The Kiteworks content firewall provides complete visibility, compliance, and control over IP, PII, PHI, and other sensitive content. It extends the Box and Microsoft offerings across all 3rd party communication channels, including email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows.

The Kiteworks platform supports SOX, GLBA, HIPAA, CMMC, GDPR, and other compliance requirements and is FedRAMP Authorized, SOC 2+ HITRUST Certified, and FIPS 140-2 Validated.



ACCELLION CUSTOMERS

TARGET · AAA · NIST National Institute of Standards and Technology U.S. Department of Commerce · Linde · KPMG · NYC HEALTH+ HOSPITALS · tyler technologies · HARTMANN · RSA · Mylan Better Health for a Better World