Kiteworks

Top 5 Microsoft 365 E3 and E5 Content Protection and Compliance Gaps Kiteworks Fills

Layer Kiteworks over your existing Microsoft 365 instance to provide the highest level of protection and compliance you can achieve with a single platform across email, file share, managed file transfer (MFT), SFTP, API integrations, and web forms.

1. Ultimate Privacy Protection With Single-tenant Hybrid Cloud Deployment Options and Customer-owned Keys

Control where your instance resides, whether on VMware, Hyper-V, AWS, Azure, Kiteworks hosted, or Kiteworks FedRAMP Moderate hosted. You always own the keys, so your data is protected from exposure to anyone other than those whom you specify, even from Kiteworks or the government via the U.S. Federal CLOUD Act. And there's no chance of a hack or leak from penetration of a shared server environment like the August 2020 Azure Cosmos DB breach because Kiteworks deploys as an independent, single-tenant cloud for each customer.

2. Broader Coverage to Include Non-Microsoft Environments and Technologies

Support Microsoft's content and ecosystem, but also your ecosystem beyond Microsoft. Govern and protect any file type used by your business processes and clients, like CAD, DNA sequences, and manufacturing equipment outputs, not just Microsoft Office and PDF. AWS and VMware, not just Azure and Hyper-V. Your security stack including DLP, ATP, authentication, HSM, CDR, SMS, SIEM, and more. And enterprise communication capabilities like SFTP and MFT, not just email and file sharing.

3. Centralized Security and Compliance Controls Across Multiple Communication Technologies

Simplify administration with a single set of roles to centrally manage user policy controls, including external parties, across email, file sharing, SFTP, MFT, and forms, instead of separate controls for each service. Define content-centric policies based on Microsoft Information Protection (MIP) labels, as well as policies based on locations, domains, users, and other factors.

4. Normalized Tracking Across Multiple Communication Technologies

Enable SecOps and simplify audit preparation with a unified, real-time, SIEM-ready log, rather than a separate log per service. It collects every user or administrative action—as well as critical system activities—unifying and standardizing them across all the connected communication channels and services for ready analysis and reporting.

5. Unlimited File Size Support

Reliably handle massive file sizes, leaving users plenty of room for CAD, video, DNA sequences, and scientific datasets and no reason to use unsanctioned workarounds.