Kiteworks

PRODUCT BRIEF

Top 5 Advantages of Kiteworks MFT Capabilities Over Axway MFT

Legacy managed file transfer (MFT) solutions have been in the market for decades to transfer sensitive files throughout organizations and with third parties. But as this content contains critical data, such as personally identifiable information (PII), corporate IP, national secrets, and more, MFT has become an increasing focus for malicious nation-states and cybercriminals. In turn, regulatory bodies have instituted various compliance controls around data privacy, security, and governance that includes MFT communications.

As a result of heightened cyber risk and compliance scrutiny, not every MFT solution meets the requirements of private and public sector organizations. There are numerous MFT solutions on the market, and a comparison with Axway MFT shows Kiteworks provides a better option for many organizations focused on security and compliance.

1. Unrivaled Software Security Hardening

Fewer than half of organizations surveyed indicate they employ a zero-trust security approach to their MFT programs.[1] This is one of the reasons MFT is becoming a growing target for cyberattacks. The Kiteworks platform employs a defense-in-depth security model using a hardened virtual appliance with a built-in network firewall, zero-management web application firewall (WAF), encryption in transit and at rest, intrusion detection, and administration access only via application user interfaces. It employs zero-trust principles that include centralized authentication integrated into all workflows, principle of least privilege, role-based policy controls, separation of administrative duties, segmentation of access to internal services, and comprehensive visibility for analytics.

The Kiteworks engineering team also oversees a bug bounty program and performs regular penetration testing to minimize vulnerabilities. For its on-premises deployments, Axway does not provide security hardening, and administrators have access to the operating system and server internals that include the file system containing the content and the database containing the metadata.

2. Comprehensive Governance Tracking and Controls

When asked to rank eight priorities involving sensitive content communications, 49% of respondents ranked unifying sensitive content communications governance and security either as their first- or second-highest priority.[2] Axway MFT components produce separate logs, which requires Axway customers to spend time and resources consolidating and standardizing the data for compliance audits and their security operations team. The Kiteworks platform centralizes governance over an organization's sensitive content communications channels with a single set of role-based policy controls. It continuously feeds syslog with comprehensive, unified, pre-standardized log entries and alerts that drive a more effective security information and event management (SIEM) system.

3. Absolute Privacy With Single-tenant Hosting

For hosted deployments, Axway, not its customers, owns the encryption keys. Axway MFT typically uses a multitenant architecture that shares OS, runtime, repositories, and file systems across all customers, with single-tenant hosting as a pricier option. Kiteworks customers that opt for a hosted application get a single

tenant that is separate from other customers by default. Moreover, Kiteworks customers—not the cloud provider—own their encryption keys, ensuring vendors and governments have no access to your content.

4. Ad Hoc Sensitive Content Communications

Axway focuses on extensive B2B integrations but offers limited content communications channel options beyond MFT. Axway Syncplicity provides file sharing options but is a cloud-only application with optional on-premises storage. Axway MFT also offers limited integration of other security investments like data loss prevention (DLP), antivirus and antispam, and advanced threat prevention (ATP). In contrast, Kiteworks has world-class sensitive content communications capabilities for email encryption, secure file sharing, and business-user-friendly SFTP in addition to MFT. This provides individual users with multiple, fully integrated options for ad hoc scenarios, and they are all governed under the same set of security and compliance policies.

5. FedRAMP Compliance

Kiteworks delivers a Private Content Network that is a simple and secure way to send, share, receive, and store PII, protected health information (PHI), and other confidential information in compliance with a long list of regulations and standards. Unique in the MFT market, Kiteworks hosts FedRAMP Moderate Authorized deployments with continuous monitoring and annual audits by a federally authorized third-party assessment organization. Further, Axway MFT's inability to deliver a centralized governance and security metadata repository across all sensitive content communications channels can be a significant challenge for many organizations.

[1] "Sensitive Content Communications Privacy and Compliance Report," Kiteworks, April 2022.
[2] Ibid.