Key Takeaways From Kiteworks' Data Security and Compliance Risk: 2025 MFT Survey Report

MFT Security Survey Findings: The 59% Problem

Kiteworks' inaugural Data Security and Compliance Risk: MFT Security Report reveals a fundamental disconnect: While companies invest heavily in perimeter defenses, their file transfer systems remain dangerously exposed. The data exposes three critical gaps driving the 59% incident rate across surveyed organizations.

Nearly 6 out of 10 organizations reported MFT security incidents in the past year.

Core Problem

Organizations have created a perfect storm of vulnerabilities through neglect of basic controls. Government agencies encrypt only 8% of stored file data. Healthcare protects just 11% despite handling our most sensitive information. Meanwhile, 26% of organizations have already experienced AI-related security incidents, with 30% permitting uncontrolled AI tool usage with MFT data. Mid-market companies (5,000-10,000 employees) face the highest breach rates at 32%, proving that size doesn't guarantee security.

Three Critical Gaps

1. The Encryption Disconnect

While 76% encrypt data in transit, only 42% protect data at rest—leaving millions of files vulnerable in storage. This 34-point gap represents the single most exploitable vulnerability, with government and healthcare showing the weakest implementation despite strict compliance requirements.

2. Security Monitoring Blindness

63% haven't integrated MFT with SIEM/SOC platforms, operating without visibility into file movements. Security teams monitor everything except the systems moving their most sensitive data, missing early attack indicators and insider threats that comprise 27% of incidents.

3. Architectural Fragmentation

62% operate separate systems for email security, file sharing, and web forms. Each additional platform multiplies attack surfaces through policy inconsistencies and integration gaps. Unified platforms show 50% fewer incidents, yet most organizations maintain this dangerous complexity.

Industry Patterns

Financial Services demonstrates what works: Balanced implementation across all controls yields a 25% incident rate, half the average. They don't excel in any single area but maintain consistency across encryption, monitoring, and governance.

Healthcare's paradox proves compliance doesn't equal security: 100% transit encryption coexists with 44% incident rates due to weak at-rest protection and fragmented systems.

Government exemplifies policy-practice disconnect: Strong frameworks meet 8% at-rest encryption, driving 50% incident rates and 25% unauthorized access attempts.

Automation Factor

Only 13% achieve 90-100% file transfer automation, yet this group shows just 29% incident rates versus 71% for those below 50% automation. Most plateau at 50-70%, missing the compounding security benefits of comprehensive automation.

Breaking the Cycle

The 39% avoiding incidents aren't perfect—they're comprehensive. They implement three fundamental controls:

- **Encrypt stored data:** Weeks to implement, immediate impact
- **Connect monitoring:** Hours to activate SIEM integration
- **Consolidate platforms:** 12- to 18-month ROI through unified architecture
- **Block AI misuse:** Deploy automated controls to prevent unauthorized AI tool access (only 44% currently protected)

Advanced protections matter too. Only 27% deploy content disarm and reconstruction (CDR) despite its effectiveness against weaponized files. The AI threat compounds this—while 48% claim to manage AI risks, the 26% already experiencing incidents proves that awareness without automated enforcement is meaningless. Vendor assessments remain superficial—72% claim thorough evaluation while 59% suffer incidents.

Reality Check

This isn't about sophisticated attacks or resource constraints. It's about organizations i`nvesting millions in advanced security while leaving fundamental gaps exposed. Every unencrypted file, every unmonitored transfer, every fragmented system compounds risk daily.

The data proves transformation doesn't require perfection—just focused action on vulnerabilities that matter most. The question isn't whether your organization can achieve better MFT security. It's whether you'll act before joining the 59% learning these lessons through incident response.

Download the MFT Report