New Survey Reveals Critical Need to Shift From Legacy Web Forms to Secure Data Forms

Kiteworks Data Forms Report Uncovers Critical Security Gaps as 44% Suffered Data Breaches Through Form Submissions and 85% Demand Data Sovereignty Controls

SAN MATEO, CA, UNITED STATES, December 4, 2025 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today released its comprehensive 2025 Data Security and Compliance Risk: Data Forms Survey Report. The research of 324 cybersecurity, risk, IT, and compliance professionals exposes a stark reality: Organizations face a critical security gap between their confidence in web form protection and actual incident rates, with sovereignty and encryption requirements driving an urgent shift from legacy web forms to secure data forms.

> Organizations collect their most sensitive information through forms yet most form solutions were built for convenience, not security. ”
>
> *Tim Freestone, Chief Marketing Officer at Kiteworks*

The survey findings paint a sobering picture of web form vulnerability in modern enterprises. Despite 64% of organizations rating their security maturity as advanced or leading, an overwhelming 88% experienced at least one web form security incident in the past two years, with 44% suffering confirmed data breaches through form submissions.

"The findings are clear. Stop using legacy web forms. Start using secure data forms," said Tim Freestone, CMO at Kiteworks. "This research reveals a fundamental truth that security leaders have suspected but couldn't quantify. Traditional web forms have become the weakest link in enterprise data protection. Organizations collect their most sensitive information through forms—financial records, health data, authentication credentials, government IDs—yet most form solutions were built for convenience, not security. The industry needs to evolve from treating forms as simple data entry tools to recognizing them as critical infrastructure requiring military-grade protection, complete data sovereignty, and continuous compliance validation."

Attack Landscape Reveals Persistent Threats
The report documents widespread and sophisticated attacks targeting web forms across all industries:

- 61% faced bot and automated attacks flooding forms with malicious traffic
- 47% experienced SQL injection attacks despite widespread adoption of parameterized queries
- 39% encountered cross-site scripting (XSS) vulnerabilities
- 28% suffered session hijacking incidents
- 21% experienced man-in-the-middle attacks

These attacks persist despite high adoption of traditional security controls. The data suggests that controls exist at the platform level but fail to achieve consistent coverage across legacy, embedded, and department-owned forms.

Data Sovereignty Emerges as Non-Negotiable Requirement
The survey's most striking finding: 85% of organizations rate data sovereignty as critical or very important, with 61% stating it is strictly required for compliance. Sovereignty requirements remain consistently high across industries—government (94%), financial services (93%), healthcare (83%), and technology (86%).

"The sovereignty findings fundamentally change the conversation around form security," said Patrick Spencer, SVP of Americas Marketing and Industry Research at Kiteworks. "Organizations cannot simply opt out of sovereign control—they must demonstrate that citizen and customer data remains within approved jurisdictions. Traditional form solutions cannot deliver these capabilities because they were never architected with multi-region isolation or government-cloud deployment in mind. The market is dividing between vendors who can prove data residency and those who cannot."

Regulatory Complexity Drives Market Segmentation
Organizations operate under multiple overlapping frameworks: 92% face GDPR requirements, 58% must satisfy PCI DSS, 41% operate under HIPAA (97% in healthcare), and 75% of government respondents require FedRAMP authorization. This regulatory convergence creates distinct market segments with sharply different security needs.

The high-security segment—government and financial services—demands FedRAMP authorization, FIPS 140-3 validated cryptography, and strict data residency controls. Government agencies require that 75% of data remains within national borders, effectively excluding vendors without government-grade certifications. Financial services faces the highest risk profile (90% collect financial records, 83% process payment cards), while healthcare handles the most sensitive data (97% collect protected health information). The research shows 71% plan upgrades within six months, driven by recent incidents (82%) and regulatory requirements (76%).

Detection-Response Gap Leaves Organizations Vulnerable
The research uncovers a critical operational gap: While 82% of organizations have real-time threat detection capabilities, only 48% have automated incident response in place. This means

approximately 34% can detect attacks in real time but still depend on manual processes—tickets, emails, and human handoffs—to contain them.

Organizations that combine real-time detection with automated response report notably lower breach rates and faster containment times. The data suggests that detection without orchestration creates dangerous delays, increasing the probability that reconnaissance attacks escalate into full data breaches.

Mobile Security Lags Despite Dominant Usage

Mobile devices now represent the primary channel for form submissions, with 71% of organizations receiving 21% to 60% of submissions from mobile devices. However, mobile-specific security controls lag significantly behind desktop protections. Only 23% rate certificate pinning as critical, and biometric authentication—adopted by 48%—is rarely enforced on high-risk flows.

This gap creates substantial risk as attackers increasingly target mobile-heavy forms such as customer identity verification, password reset workflows, benefits enrollment, and service portals where sensitive data combines with weaker client-side defenses.

Key Recommendations for Enterprise Security Leaders

The report provides strategic recommendations for reducing form-related risk, including:

- Centralize governance across all forms to enforce uniform security standards
- Enforce end-to-end encryption with FIPS 140-3 validation and field-level encryption
- Implement data sovereignty controls with flexible deployment options
- Pair real-time monitoring with automated incident response
- Automate compliance evidence generation

The complete 2025 Data Forms Survey Report is available here.

About Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a Private Data Network that delivers data governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and over 1,500 global enterprises and government agencies. Learn more at www.kiteworks.com.

David Schutzman
Kiteworks
+1 203-550-8551
email us here
Visit us on social media: