Kiteworks Survey Reveals Only 17% of Organizations Have Technical Controls for AI Data Security

Organizations rush to adopt AI but fail to have commensurate security and compliance controls in place

SAN MATEO, CA, UNITED STATES, June 16, 2025 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today released findings from its AI Data Security and Compliance Risk Survey of 461 cybersecurity, IT, risk management, and compliance professionals. The survey, which was conducted by Centiment, reveals critical implementation failures: Only 17% of organizations have technical controls that block access to public AI tools combined with DLP scanning, while 26% report over 30% of data employees ingest in public AI tools is private data.

> The data reveals organizations significantly overestimate their AI governance maturity."
>
> *Tim Freestone, Chief Marketing Officer at Kiteworks*

These findings emerge amid a documented surge in AI-related incidents. Stanford's 2025 AI Index Report records a 56.4% year-over-year increase in AI privacy incidents, reaching 233 incidents last year.[1] The Kiteworks survey exposes how organizations remain unprepared: 40% restrict AI tool usage through training and audits, 20% rely solely on warnings without monitoring, and 13% lack any specific policies for public AI tool usage—leaving the vast majority vulnerable to emerging threats.

"Our research reveals a fundamental disconnect between AI adoption and security implementation," said Tim Freestone, Chief Marketing Officer at Kiteworks. "When only 17% have technical blocking controls with DLP scanning, we're witnessing systemic governance failure. The fact that Google reports 44% of zero-day attacks target data exchange systems undermines the very systems organizations rely on for protection."

Industry Benchmarks Reveal Dangerous Overconfidence Gap

The Kiteworks survey exposes a critical overconfidence crisis in AI governance readiness. While one-third of survey respondents claim they have comprehensive governance controls and tracking in place, this contrasts starkly with Gartner's finding that only 12% of organizations have

dedicated AI governance structures, with 55% lacking any framework whatsoever.[2] This dramatic gap between perception and reality creates unprecedented risk exposure.

Deloitte's research provides even more sobering context: Only 9% of organizations achieve "Ready" level AI governance maturity, despite 23% claiming to be "highly prepared"—a 14-point overconfidence gap.[3] This misalignment is particularly concerning given that 86% of organizations lack visibility into AI data flows, according to industry research.[4]

The rush to adopt AI without proper controls is accelerating. A recent EY survey found 48% of technology companies are already deploying AI agents, with 92% planning to increase AI spending—a 10% jump from March 2024.[5] Yet this enthusiasm comes with what EY calls "tremendous pressure" to demonstrate ROI, creating incentives to prioritize speed over security.

"The gap between self-reported capabilities and measured maturity represents a dangerous form of organizational blindness," explained Patrick Spencer, VP of Corporate Marketing and Research at Kiteworks. "When organizations claiming governance discover their tracking reveals significantly more risks than anticipated according to Deloitte, and when 91% have only basic or in-progress AI governance capabilities, this overconfidence multiplies risk exposure precisely when threats are escalating."

Legal Sector Exemplifies Implementation-Awareness Gap

The Kiteworks survey found legal professionals report the highest concern about data leakage at 31%, yet implementation remains weak: 15% have no specific policies or controls regarding the use of public AI tools with company data, while 19% rely on unmonitored warnings.

This implementation gap becomes more pronounced in privacy investment strategies. While 23% of all organizations maintain comprehensive privacy controls with regular audits before any AI system deployment, only 15% of legal firms have fallen into the trap of having no formal privacy controls while prioritizing rapid AI adoption—an 8-point improvement over the 23% average across all sectors yet still concerning given their fiduciary duties.

The disconnect aligns with Thomson Reuters data showing only 41% of law firms have AI policies despite 95% expecting AI to become central within five years.[6] This gap between current readiness and future expectations in the legal sector—an industry built on precedent and risk mitigation—exemplifies the broader organizational tendency to defer critical security implementations while embracing transformative technologies.

AI Security Gap: When Perception Meets Reality

The survey's finding that only 17% have implemented technical controls that block access to public AI tools combined with DLP scanning becomes more concerning given the evolving threat landscape. Google's research reveals 44% of zero-day vulnerabilities target data exchange systems, with 60% of enterprise-targeted zero days exploiting security and networking

tools—the very systems meant to protect sensitive data.

Despite awareness of risks, the Kiteworks survey found organizations remain deeply divided on addressing vulnerabilities:
- 34% report using a balanced approach with data minimization and selective privacy-enhancing technologies
- 23% maintain comprehensive privacy controls with regular audits
- 10% have basic privacy policies but prioritize AI innovation
- 10% address privacy concerns reactively, focusing on compliance only when legally required
- 23% have no formal privacy controls and prioritize rapid AI adoption

Based on the convergence of weak controls, limited visibility, and escalating threats, organizations must:
1. Acknowledge Reality: Recognize that self-assessed governance may significantly overstate actual maturity based on industry benchmarks
2. Deploy Verifiable Controls: Implement automated governance tracking and controls that can demonstrate compliance, not just claim it
3. Prepare for Regulatory Scrutiny: Quantify exposure gaps and implement measurable improvements

"The data reveals organizations significantly overestimate their AI governance maturity," concluded Freestone. "With incidents surging, zero-day attacks targeting the security infrastructure itself, and the vast majority lacking real visibility or control, the window for implementing meaningful protections is rapidly closing."

For the entire report, download a copy.

[1] “The 2025 AI Index Report,” Stanford University, 2025.
[2] “AI Governance Frameworks for Responsible AI,” Gartner, March 20, 2023.
[3] “New Deloitte survey finds expectations for Gen AI remain high, but many are feeling pressure to quickly realize value while managing risks,” Deloitte, January 15, 2024.
[4] “Flying blind: Only 14 percent of companies surveyed have a comprehensive overview of generative AI usage,” LeanIX, June 18, 2024.
[5] “EY survey reveals that technology companies are setting the pace of agentic AI – will others follow suit?” EY, May 14, 2025.
[6] “2025 Generative AI in Professional Services Report,” Thomson Reuters, February 2025.

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.

About Centiment
Centiment is a market research firm specializing in data collection and analysis for the cybersecurity and technology sectors. The company delivers actionable insights through customized survey design, targeted respondent recruitment, and sophisticated analytics. Centiment's proprietary research platform ensures exceptional data quality through expert human oversight. The company serves Fortune 500 enterprises, technology vendors, and government agencies, providing intelligence for strategic decisions in evolving markets. Headquartered in Denver, Centiment conducts research globally to help organizations understand complex technology landscapes and cybersecurity trends.

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