New Research: Europe's AI Security Controls Trail Global Benchmarks as Attack Surface Expands

France, Germany, UK all lag on AI anomaly detection (40% global). Training-data recovery trails by 7 points. Europe regulates AI—but can't secure it.

LONDON, UNITED KINGDOM, January 6, 2026 /EINPresswire.com/ -- Kiteworks, which empowers organisations to effectively manage risk in every send, share, receive, and use of private data, today released its Data Security and Compliance Risk: 2026 Forecast Report. The comprehensive analysis reveals that European organisations trail global benchmarks on the security controls needed to detect AI-specific threats, respond to AI-enabled breaches, and govern AI data flows.

> When an AI model starts behaving anomalously, European organisations are less equipped than their global counterparts to detect it. That's not a compliance gap. That's a security gap."
>
> *Wouter Klinkhamer, GM of EMEA Strategy & Operations, Kiteworks*

The research, based on a survey of security, IT, compliance, and risk leaders across 10 industries and 8 regions, exposes a widening gap between Europe's regulatory leadership, with regulations such as the EU AI Act, and its actual AI security posture. European organisations trail on AI anomaly detection (France 32%, Germany 35%, the UK 37% vs. 40% global), training-data recovery (40% to 45% vs. 47% global), and software bill of materials (SBOM) visibility for AI components (20% to 25% vs. 45%+ in leading regions). When AI systems behave unexpectedly—or when AI-enabled attacks target European infrastructure—most organisations lack the detection capabilities to identify the threat. This can result in compliance fines and negative brand exposure as well as breaches of sensitive data.

"Europe has led the world on AI governance frameworks—the AI Act is setting the global standard for responsible AI deployment. But governance without security is incomplete," said Wouter Klinkhamer, GM of EMEA Strategy & Operations, Kiteworks. "When an AI model starts behaving anomalously—accessing data outside its scope, producing outputs that suggest compromise, or failing in ways that expose sensitive information—European organisations are less equipped than their global counterparts to detect it. That's not a compliance gap. That's a security gap."

The report identifies five predictions for European organisations in 2026:

1. AI-specific breach detection will lag other regions. France (32%), Germany (35%), and the UK (37%) all trail the 40% global benchmark on AI anomaly detection—the capability to identify when AI models behave unexpectedly. When AI-enabled attacks exploit model vulnerabilities or AI systems access data outside their intended scope, European organisations will be slower to detect the breach, exacerbating the detrimental impact of the exposure.

2. AI incident response will remain incomplete. Training-data recovery—the ability to diagnose AI failures by examining what the model learned from—sits at 40% to 45% across Europe versus 47% global and 57% in Australia. Without this capability, organisations can't forensically analyse AI incidents or prove what went wrong to regulators.

3. AI supply chain visibility will remain a blind spot. SBOM adoption for AI components sits at 20% to 25% across Europe versus 45%+ in leading regions. Organisations can't secure AI models built on third-party components they can't see. As attackers increasingly target vulnerabilities in AI libraries, datasets, and frameworks, this visibility gap stops being a compliance checkbox and becomes an open door. Organizations without component inventories can't detect exposure, can't trace compromise origins, and can't respond until damage is already done.

4. Third-party AI vendor incidents will catch organizations unprepared. Only 4% of French organizations and 9% of UK organizations have joint incident response playbooks with their AI vendors. When a vendor's AI system is compromised—and that compromise flows into European infrastructure—organizations won't have the detection mechanisms, communication channels, or containment protocols in place. The breach spreads before they know it exists.

5. AI governance evidence will remain manually generated. European organizations cluster in "continuous but manual" compliance rather than automated evidence generation. This creates dual financial exposure: Regulators assessing fines will find documentation that is slow to produce and inconsistent in quality, while insurers adjudicating breach claims may deny coverage entirely if organizations cannot demonstrate adequate AI governance controls were in place. Governance thus becomes a payout gap.

The implications extend beyond compliance. AI systems are increasingly processing sensitive data, making autonomous decisions, and integrating with critical infrastructure. Every AI model that can't be monitored for anomalies is a system where adversarial inputs, data poisoning, or model manipulation go undetected. Every third-party AI component that can't be tracked is a dependency where upstream compromises silently inherit into your environment. Every AI vendor relationship without a joint incident playbook is a breach that spreads unchecked across organizational boundaries.

These aren't governance failures waiting for a regulatory audit. They're attack surfaces waiting for an adversary. Compliance gaps carry the abstract risk of penalties. Security gaps carry the

concrete certainty of compromise—data exfiltration, manipulated outputs, operational disruption. The difference is between a fine you can budget for and a breach you can't predict.

The global report, which includes 15 predictions across data visibility, AI governance, third-party risk, and compliance automation, identifies "keystone capabilities"—unified audit trails and training-data recovery—that predict success across all other security metrics, showing a measurable advantage for organisations that have implemented them.

"The AI Act establishes what responsible AI governance looks like. The question for European organisations is whether they can secure what they're governing," said Klinkhamer. "By end of 2026, the organisations that have closed the gap between AI policy and AI security—anomaly detection, training-data recovery, supply chain visibility, vendor incident coordination—will be positioned for both compliance and resilience. Those still running AI workloads without detection capabilities will learn about their security gaps the hard way: from attackers, not auditors."

Download the full 2026 Forecast Report here and the European brief on the report here.

About Kiteworks
Kiteworks' mission is to empower organisations 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 organisation, 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.

Martin Brindley
Martin Brindley PR Ltd
1256 762811
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X