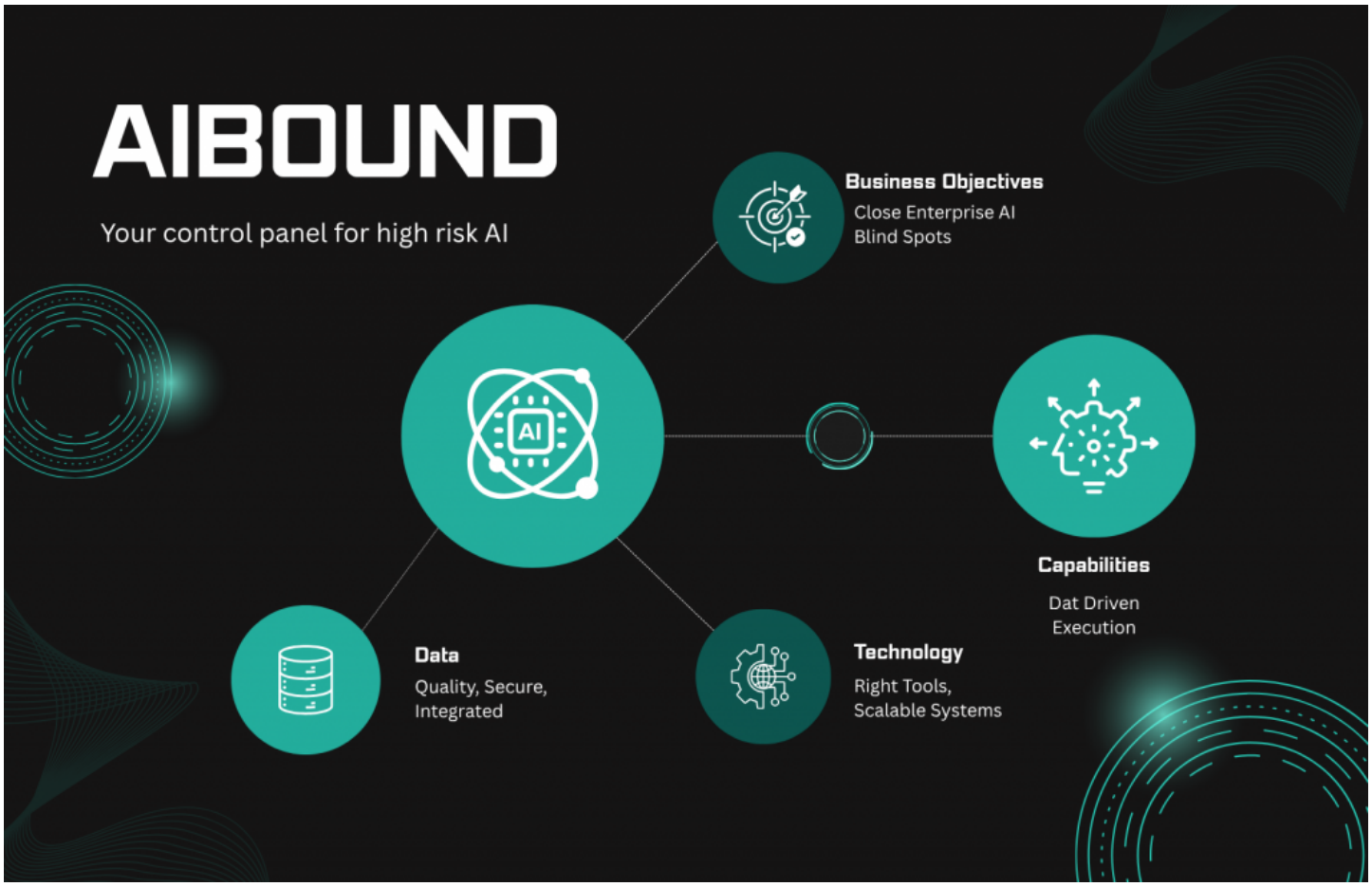
AIBound Highlights Enterprise AI Visibility Gap as EU AI Act Enforcement Begins

As the EU AI Act moves into active enforcement, AIBound is helping enterprises establish the AI inventory, risk context, and policy visibility needed to govern AI use across browser, endpoint, network, and cloud environments.



San Mateo, California Aug 18, 2026 (Issuewire.com) - AIBound, an enterprise AI security company, today highlighted a growing readiness problem facing organizations operating under the European Union's AI Act: many enterprises are being asked to govern AI systems they cannot yet reliably see, classify, or track.

The EU AI Act became generally applicable on August 2, 2026, with transparency requirements and enforcement mechanisms now active and additional high-risk requirements following phased implementation dates. For security, legal, risk, and compliance teams, that shifts AI governance from a future planning exercise into an operational requirement. Before an organization can determine which obligations apply to a system, it first needs to know what AI is being used, where it is running, what data it can access, and whether that use is sanctioned.

The Compliance Problem Starts With Visibility

Enterprise AI adoption has moved faster than the governance systems built to manage it. Employees can introduce new AI tools in minutes, SaaS platforms increasingly embed AI features by default, and

autonomous agents can act through existing enterprise identities and data connections. The result is a fragmented environment in which the systems subject to governance may not appear in one authoritative inventory.

IBM's 2025 Cost of a Data Breach Report found that 63 percent of breached organizations either had no AI governance policy or were still developing one. One in five organizations reported a breach involving shadow AI, while only 37 percent had policies to manage AI or detect unsanctioned AI use. Organizations with high levels of shadow AI also saw breach costs average $670,000 more than those with little or no shadow AI.

The regulatory market is moving in the same direction. Gartner reported in February 2026 that spending on AI governance platforms is expected to reach $492 million in 2026 and exceed $1 billion by 2030, as organizations look for centralized oversight and continuous compliance across expanding AI estates.

From AI Inventory to Risk Classification

AIBound's AI Control Plane is designed to give enterprises a current view of AI activity across their existing environment. The platform discovers sanctioned and unsanctioned AI, identifies the identities under which AI agents operate, maps data connections, and assigns risk grades across more than 50,000 cataloged AI applications, agents, models, and services.

That visibility gives governance teams a practical starting point for EU AI Act readiness. Instead of relying on manual questionnaires or periodic inventories, organizations can use observed AI activity to support internal classification, authorization, policy enforcement, and evidence collection.

- Discover AI tools and agents as they appear across the enterprise environment
- Identify the user, service account, or agentic identity associated with AI activity
- Map the data and systems each AI tool can reach
- Apply consistent risk grading to help prioritize review and governance
- Feed AI risk signals into existing security, SIEM, and GRC workflows

Built to Fit Existing Enterprise Security Workflows

AIBound connects to more than 100 enterprise security tools without requiring new endpoint agents or major infrastructure changes. Organizations can establish an AI inventory and risk view using telemetry already available across browser, endpoint, network, cloud, and security platforms.

AIBound is SOC 2 and ISO 27001 certified and is designed to support governance programs aligned with the EU AI Act and the NIST AI Risk Management Framework. The platform does not replace legal interpretation or formal compliance assessment; it provides the technical visibility and risk context those processes increasingly depend on.

[EMEA PARTNER QUOTE TO BE INSERTED BEFORE DISTRIBUTION: Recommended angle - the practical challenge is not understanding the regulation in theory, but proving which AI systems are actually in use and bringing them into a repeatable governance process.]

A Readiness Layer for the AI Era

As AI regulation matures, enterprises will need to move from policy documents to continuously verifiable controls. That begins with a simple question: can the organization produce a reliable, current view of the

AI systems operating across its environment?

For AIBound, the answer is to make AI itself visible as an enterprise asset and risk surface. By creating a common inventory and classification layer, security and compliance teams can evaluate AI use with the same operational discipline they already apply to identities, endpoints, applications, and data.

About AIBound

AIBound is the AI Control Plane for enterprise security. The platform enables security teams to discover shadow AI, expose agentic identities, map data connections, score risk, and enforce policy across browser, endpoint, network, and cloud, without deploying new agents or disrupting existing infrastructure. AIBound is SOC 2 and ISO 27001 certified and integrates with more than 100 enterprise tools. The company is headquartered in San Mateo, California, with offices in the United Kingdom, India, and South Africa. For more information, visit www.aibound.com.

Editorial source references: European Commission, EU AI Act implementation timeline; IBM Cost of a Data Breach Report 2025; Gartner, Global AI Regulations Fuel Billion-Dollar Market for AI Governance Platforms, February 2026.

Media Contact

AIBound

*********@aibound.com

https://www.aibound.com/

Source : AIBound