

Enabling Secure AI Adoption



Where Mobility and AI Converge

The rapid rise of artificial intelligence (AI), combined with widespread mobile adoption, is fundamentally reshaping how work gets done—and, in parallel, redefining how risk emerges and spreads across the enterprise.

With 93% of surveyed organizations reporting employee use of generative AI on mobile devices, mobile has become a primary surface for AI interaction—yet it remains largely invisible. Existing discovery approaches rely on network gateways to inspect traffic and identify AI activity by analyzing API signatures and protocol patterns. But when employees access AI tools such as ChatGPT, Claude, and Gemini directly on mobile devices, that traffic often bypasses these controls entirely—leaving mobile environments a persistent, largely unmonitored blind spot.

AI Isn't Waiting for Governance to Catch Up

Enterprise AI adoption isn't just centrally orchestrated. It is emerging organically from the ground up. Employees are rapidly experimenting with AI tools, integrating them into everyday workflows, and driving productivity gains, often without formal approval or oversight.

This dynamic has fueled the rise of “Shadow AI,” in which employees use unsanctioned AI applications without IT visibility or control. The result is a fundamental gap in which sensitive corporate data is accessed, processed, or stored by AI services operating outside established security boundaries. With 78% of knowledge workers already using personal AI tools for work, this is no longer an edge case. It is a rapidly expanding, largely unmanaged attack surface.

And the Problem is Compounding

The security challenge intensifies as we enter the era of Agentic AI. Unlike Generative AI, agentic systems are “autonomous actors” that plan, decide, and execute multi-step workflows independently. Agentic usage is growing rapidly, with Gartner estimating that by the end of 2026, more than 40% of enterprise applications will include task-specific AI agents. These systems can autonomously initiate communications, trigger financial transactions, and modify records without human oversight. With over 25,000 AI-enabled apps already in major app stores, employees can instantly deploy these autonomous capabilities at the mobile edge.

The Conventional Playbook Falls Short

While traditional security controls remain essential to a defense-in-depth strategy, they rely on visibility and control capabilities that are primarily available in desktop and cloud environments. In those domains, security tools can deeply inspect traffic and observe user interactions at a granular level. Mobile platforms operate differently. The app-centric architecture of iOS and Android enforces strict sandboxing and privacy boundaries, limiting cross-app visibility and preventing the kind of traffic interception and inspection common on Windows or in managed cloud infrastructure.

Governing AI on mobile, therefore, requires a different approach. Instead of focusing on the device, the focus shifts to understanding application behavior. The Lookout platform performs deep structural and functional analysis of mobile applications. By examining how apps are built and how they behave, it identifies which apps embed AI capabilities, traces data flows when those capabilities are used, and detects whether sensitive information, such as location or contacts, is shared with AI endpoints.

This level of intelligence gives security teams the context to act. Organizations can define policies to allow, restrict, or redirect application behavior, establishing the visibility and control needed to govern AI adoption across the mobile fleet.

A Purpose-Built Approach to Mobile AI Visibility & Governance

Organizations must ensure they use the right tools for a mobile environment. To be effective, the solution must align with the architecture and constraints of mobile platforms rather than relying on mechanisms designed for desktop and cloud environments. This requires a purpose-built approach to Mobile AI Visibility and Governance grounded in a set of foundational capabilities:

- **AI App Discovery & Shadow AI Visibility:** Real-time inventory of all AI-enabled apps, exposing unsanctioned use and bringing hidden mobile risk under control.
- **Agentic Behavior Monitoring:** Continuous analysis of AI-driven activity to prevent unauthorized actions and data access.
- **Data Guardrails & Policy Enforcement:** Real-time controls to stop sensitive data exposure and exfiltration to unapproved AI services.
- **Automated Compliance Alignment:** Audit-ready reporting aligned to ISO/IEC 42001, the EU AI Act, and NIST AI RMF.

These are not incremental improvements; they reflect recognition that mobile architectures are fundamentally different. The operating model, visibility constraints, and control points that exist in desktop and cloud environments do not translate to mobile. As a result, effective governance requires a shift in approach, one built around how mobile platforms actually function, rather than attempting to extend legacy assumptions into an environment where they no longer apply.

Why Lookout

Mobile operates in a fundamentally different environment from traditional desktop and cloud infrastructures, where the enterprise perimeter is clearly defined and enforceable. It exists outside those conventional boundaries, beyond network perimeters, gateways, and most enterprise discovery tools, making an increasing share of AI activity effectively invisible. As employees engage with AI agents and services directly through mobile apps, that usage often bypasses the telemetry and enforcement points that underpin existing governance strategies. The result is a material gap: organizations may believe they have comprehensive AI oversight, while a meaningful portion of real-world usage remains unseen and unmanaged.

This is precisely where Lookout delivers differentiated value. Built natively for mobile, the platform provides visibility at the application layer, where AI interactions occur. By analyzing how apps are built and how they behave, Lookout uncovers embedded AI capabilities, traces data flows to AI endpoints, and identifies when sensitive information is exposed. This approach restores the visibility and control needed to govern AI effectively in a mobile-first world, closing the gap left by traditional security models.

Conclusion

AI is reshaping the enterprise, and mobile is where that shift is most evident. As AI moves into mobile apps, visibility gaps widen, leaving organizations unable to fully manage risk, protect data, or meet compliance requirements.

Mobile AI Visibility and Governance is not merely an enhancement to existing security. It is a foundational requirement for safely adopting AI at scale.

About Lookout

Lookout, Inc. is a leader in mobile-centric security, purpose-built for the convergence of mobile and AI. Backed by more than 15 years of specialized expertise and one of the industry's most comprehensive mobile threat telemetry datasets, Lookout empowers organizations to secure and govern the modern, mobile-driven enterprise.

By delivering deep visibility into mobile endpoints, applications, network traffic, and AI-driven interactions, Lookout enables organizations to detect threats earlier, enforce policies in real time, and protect sensitive data wherever work happens. Its platform extends beyond traditional device security to address human-targeted threats, application-layer risk, and the growing impact of autonomous AI systems—helping enterprises reduce risk, maintain compliance, and operate with confidence in an increasingly mobile and AI-powered world.

Learn more at www.lookout.com and follow us on the [Lookout Blog](#), [LinkedIn](#), and [X](#).

© 2026 Lookout, Inc. LOOKOUT® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, and PROTECTED BY LOOKOUT.



Request a demo at
www.lookout.com/request-a-demo