Lookout

Mobile Threat of the Month

March 2026

The Risk of Shadow AI on Mobile

As artificial intelligence increasingly automates business workflows, organisations face a rapidly growing threat known as "Shadow AI"—the unsanctioned use of AI applications by employees without IT or security oversight. Mobile devices act as a massive force multiplier for this risk. Smartphones and tablets are the operational nerve centres of modern enterprises, concentrating identity, messaging, and cloud access into a single endpoint. The threat is compounded by the rapid influx of AI-powered applications on mobile platforms.

Potential Business Impact

The uncontrolled use of Shadow AI on mobile devices creates profound governance, security, and compliance impacts for organisations:

- **Autonomous Data Leakage:** Unsanctioned AI assistants with access to corporate emails and cloud storage can autonomously summarise and transmit sensitive materials (e.g., financial reports or board documents) to external, unvetted AI services, removing data from controlled environments.
- **Severe Compliance Exposure:** Shadow AI erodes an organisation's ability to maintain oversight over its data. This directly conflicts with emerging global governance frameworks like ISO/IEC 42001 (the international standard for AI Management Systems), which require clear governance and auditability of AI usage.
- **Blind Spots in Traditional Security:** Conventional security controls were designed for desktop and network monitoring. They are largely blind to Shadow AI activity occurring entirely within encrypted app ecosystems on mobile endpoints, leaving organisations completely unaware of the data exfiltration and unsanctioned automation happening right in their employees' hands.

Lookout Mobile Security

To combat the unique threats posed by mobile Shadow AI, organisations must adopt mobile-native security strategies. Mitigating these risks requires moving beyond traditional malware identification to comprehensive, AI-aware mobile endpoint security:

- **Total Application Visibility:** Lookout provides the capability to identify and classify which mobile applications—across both corporate and BYOD (Bring Your Own Device) environments—incorporate AI engines, uncovering the 25,000+ AI tools already in the wild.
- **Behavioural Analysis and Monitoring:** Organisations can detect unsanctioned or high-risk AI usage by monitoring data flows between AI applications and enterprise systems. This allows security teams to catch agentic, autonomous behaviours before sensitive data leaves the device.
- **Direct Policy Enforcement:** By bridging the gap between mobility and AI oversight, Lookout enables security teams to enforce governance controls and establish traceable audit trails directly at the mobile endpoint. This ensures that enterprise mobile environments align with regulatory frameworks like ISO 42001.

Source: Unite. AI