Mobile AI Governance

Exposing and Controlling Shadow AI Risk in the Enterprise

www.zimperium.com

ZIMPERIUM®

Executive Summary

As mobile devices become the primary endpoint for employee productivity, the rapid proliferation of generative AI has introduced a critical governance blind spot: Shadow AI. With over 90% of employers reporting that employees are using unsanctioned personal AI accounts for work, organizations face escalating risks of proprietary data loss, excessive mobile app permissions, and regulatory non-compliance. Current security perimeters often fail to account for AI features embedded within seemingly benign mobile applications or the use of foreign-developed AI agents. To mitigate these threats, leadership must move beyond simple domain blocking toward a robust Mobile AI Governance strategy. By leveraging deep run-time analysis and vetting of mobile apps, enterprises can gain the necessary visibility to enforce AI usage policies, protect intellectual property, and ensure the mobile fleet remains a secure asset rather than a liability.

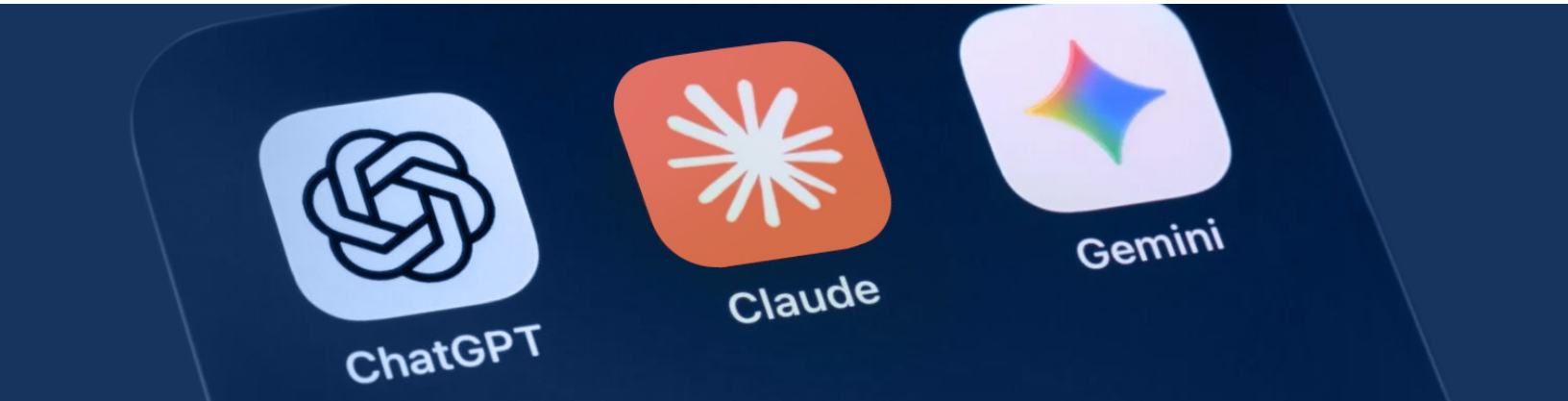
Introduction

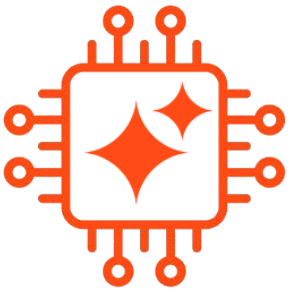
With the proliferation and use of AI in both approved and shadow IT services, enterprises can add a new challenge: unsanctioned or "Shadow AI". Employee use of public AI LLM models and bots is widespread: a 2025 MIT study found that over 90% of companies have workers using personal chatbot accounts for daily work tasks without IT approval.

Defining the Challenge: What is Shadow AI?

Shadow AI is commonly understood as the use of unsanctioned AI tools (often LLMs), applications with AI-based features, or AI agents without IT/security approval. This unsanctioned use is a blind spot for an organization and increases regulatory compliance risk (e.g. HIPAA, PCI, GDPR, etc.), intellectual property loss risk, and data breach risk.

There are two types of shadow AI use that are of concern on mobile devices: purpose-built AI apps, such as ChatGPT, Gemini and Claude, and mobile apps that embed AI, either openly or (more concerning for security teams) in a clandestine manner.





Embedded AI

Embedded AI refers to AI features that are integrated directly into mobile apps — often without user or organizational awareness and IT oversight. Applications previously approved by an organization may introduce AI functionality through routine software updates without undergoing a new security review. In just the last 9 months Zimperium's zLabs has seen a 10x increase of AI usage in mobile apps.

The risk from lack of visibility into embedded AI use by mobile apps means organizations may not know what AI service and model is being used, how it interacts with sensitive data, where the AI model is geographically located, or whether it complies with security and privacy standards. If the organization does not know these details of AI use how can it perform a cybersecurity risk review for regulatory violations?

AI Browsing and LLM Apps

The use of AI-powered browsing agents and apps (e.g., ChatGPT Agent, Microsoft Copilot, Claude, etc.) on mobile devices is a second shadow AI threat on mobile devices. Often organizations will approve one LLM service for employee use but they often have no visibility into what additional LLM apps are in use on employee mobile devices.

The Core Problem and Key Risks

So what are the risks from Shadow AI use on mobile devices? In short, shadow AI creates a "black hole" for data loss on corporate and personal mobile devices. These risks can be grouped into three categories.

Risk 1:

Data and Intellectual Property (IP) Loss: Employees exposing proprietary data such as source code, business plans, and client data by pasting it into AI prompts that they leverage for productivity. This enterprise data can then lead to the public use of proprietary data, compromising competitive advantage and R&D investment.

Risk 2:

Mobile App Data Exposure: Unsanctioned mobile apps, particularly those with embedded AI, often leverage excessive and non-compliant device permissions to exfiltrate sensitive data, turning the mobile endpoint into an unmonitored point of leakage.

Mobile apps can access a lot of data on the device through what are known as "permissions" and these permissions are often excessive. Examples of excessive permissions can often include full access to employee Contact data, Microphone & Camera Access, Files & Photos access, and User Input access. These permissions open up the device to data loss or leakage. The FBI has publicly warned of the risk of foreign-developed mobile apps leading to data exfiltration and device compromise.

Risk 3:

Legal and Compliance Failures: Failure to ensure corporate and client data is protected from unsanctioned AI use increases the risk of both legal and regulatory compliance issues. Organizations operating under requirements for controls to demonstrate compliance (identification and enforcement) must be extended to mobile devices.

The root cause of these three risks are unrestricted access to AI tools coupled with increased productivity pressure on employees and inconsistent AI policy usage enforcement on mobile devices.

Solution:
A Comprehensive Approach to Mobile AI Security

The solution to these three threats is visibility on what AI apps and AI-embedded apps are in use on mobile devices coupled with mobile AI policy enforcement. Additionally, organizations need to understand where AI is sending their data geographically and whether it complies with their data sovereignty policy.

This visibility is achieved via implementation of robust mobile app analysis and vetting coupled with policy enforcement. The key minimum features to accomplish this include:

- Identification of third-party applications using AI capabilities, whether openly or covertly
- Policy implementation of app permissions as well as the location of where apps are communicating, including foreign countries
- Implementation of controls to block unsanctioned AI tools on both corporate and employee-owned mobile devices
- Implementation of controls to ensure app permissions do not exceed necessary use and violate policy
- Enforcement of conditional access to resources only when the mobile device is in a compliance state

How Zimperium Manages Mobile AI and Closes the Shadow AI Blindspot

Zimperium's deep mobile expertise and industry-leading on-device app analysis and vetting capabilities provide the proven intelligence necessary for organizations to maintain robust mobile AI governance. Zimperium MTD includes the industry's most robust and feature-rich *mobile app vetting (MAV)* solution. Zimperium MAV helps identify and block these threats by applying App Policies and AI-specific web content filtering to mobile devices. App Vetting alerts shadow AI use on employee devices, whether AI is embedded within an app or the app itself is purpose-built for AI. Unlike solutions that may rely only on static analysis or simple domain blocking, Zimperium MAV performs deep run-time analysis to identify AI SDKs, permissions, and data flows, ensuring *true* shadow AI discovery. With Zimperium, security teams can see which AI apps are in use, what data they access, and the risk each introduces. They can then use the **Zimperium** policy engine to mark these apps as non-compliant and restrict or remove enterprise access to reduce risk before it becomes an incident. **The policy engine fully supports the ability to enforce data sovereignty requirements.**

Conclusion: Implement a Mobile AI Governance Strategy Today

It is now an imperative to broaden your security and risk policies to include use of AI from mobile devices. The importance of addressing shadow AI to protect mobile fleets and corporate assets can not be overstated. Leveraging Zimperium MTD with Zimperium mobile app vetting provides the organization with the most robust toolset in the industry to secure mobile, reduce risk and comply with governance requirements.

About Zimperium

Zimperium is the world leader in AI-Empowered mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous security that counters evolving threats including mishing, malware, and zero-day attacks.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244