carahsoft

Lookout™

Your business has a Shadow AI problem. It's on mobile.

Closing the governance gap for shadow AI and agentic systems

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Lookout, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/LookoutResources

Join Events & Webinars:
carah.io/LookoutEvents

Discover Technology Solutions:
carah.io/Lookout

Learn About Procurement:
carah.io/LookoutContracts

Connect With Our Team:
Lookout@carahsoft.com
(844) 445-5688

Lookout

Your business has a Shadow AI problem. It's on mobile.

Closing the governance gap for shadow AI and agentic systems

The AI Visibility Gap

Mobile devices now account for 52% of all Generative AI usage. There is a significant security risk as 78% of workers use personal AI tools for professional tasks, and 40% of files uploaded to these services contain sensitive corporate data.

52% of all Generative AI usage now occurs on mobile devices.

78% of knowledge workers use personal AI tools for professional tasks (BYOAI).

77% of employees admit to pasting corporate data into GenAI tools.

40% of files uploaded to AI services contain sensitive corporate information.

Beyond Generative—The Rise of Agentic AI

By the end of 2026, over 40% of enterprise applications are expected to include task-specific AI agents. These autonomous actors pose a threat because they inherit user identities and OAuth tokens, allowing them to exfiltrate data at machine speed if a security gap exists.

AUTONOMOUS ACTORS

By the end of **2026**, **more than 40%** of enterprise apps will include **task-specific AI agents**.

FULL AUTHORITY

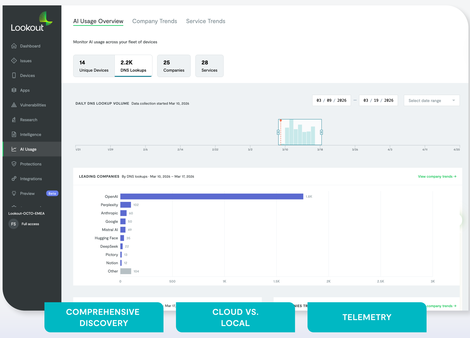
On **mobile**, these agents inherit a user's **MFA-validated identity** and **OAuth tokens** to act on their behalf.

THE THREAT

A single gap allows an agent to **exfiltrate data** or **invoke privileged APIs** at **machine speed**.

The Lookout Solution

Lookout provides a dashboard for comprehensive discovery and classification of AI-enabled apps across corporate and personal devices. It monitors telemetry and DNS lookups to track whether AI processing is occurring locally on the device or in the cloud.



COMPREHENSIVE DISCOVERY

Identify and classify AI-enabled apps across corporate and BYOD devices.

CLOUD VS. LOCAL

Track if AI processing is happening on the device or in the cloud.

TELEMETRY

Monitor DNS lookups (e.g., **1.7M lookups across 278K devices**) to measure true utilization.

Policy Enforcement and Compliance

The platform offers granular control to allow sanctioned tools like ChatGPT Enterprise while blocking unauthorized ones. It uses data guardrails to prevent exfiltration and automatically aligns mobile fleet activity with regulations like the EU AI Act.

Allow: Chat GPT Enterprise

Monitor: Gemini Usage

Block: DeepSeek or other unsanctioned tools

Granular Control: Apply specific policies

Data Guardrails: Prevent unauthorized exfiltration between mobile devices and AI services.

Automated Alignment: Directly align mobile fleet activity with ISO/IEC 42001 and the EU AI Act.

Why Lookout?

Lookout is built specifically for iOS and Android architectures rather than being a desktop retrofit. It utilizes behavioral analysis and permission mapping to ensure autonomous agents do not execute unsanctioned workflows.

	Lookout Mobile-Native	Legacy Desktop-Centric
Native Intelligence: Built for the unique architectures of iOS and Android, not a retrofit of desktop tools.	✓	✗
Behavioral Analysis: Uses permission mapping to ensure autonomous agents don't execute unsanctioned workflows.	✓	✗
Layered Defense: Integrates with Social Engineering Protection to secure both human and non-human AI actors.	✓	✗

Learn more at Lookout.com/AI-Visibility

Lookout