

SHADOW AI VISIBILITY SERVICE

Discover the AI tools and agents running
across endpoint, cloud, and SaaS.



Shadow AI is expanding faster than security teams can track.

As organizations accelerate GenAI adoption, security teams are losing visibility into what AI is actually running across the business. Employees use unsanctioned AI tools, install AI browser extensions, and leverage unapproved GenAI features in SaaS applications, creating a "shadow AI" footprint that bypasses governance and may expose sensitive data. Even sanctioned AI presents a significant challenge; security and IT teams often find it difficult to maintain an accurate inventory as AI features are frequently bundled into existing tools via license updates or enabled within SaaS platforms without formal change control. In many cases, the actual number of agents in production can vastly exceed approved use cases.

The CrowdStrike Shadow AI Visibility Service provides targeted, platform-driven discovery to reveal this hidden landscape. Powered by the CrowdStrike Falcon® platform, CrowdStrike experts identify sanctioned and unsanctioned AI across the cloud, SaaS, and endpoint planes. This visibility enables you to shift from a reactive posture to proactive defense by delivering a validated inventory of AI usage to inform governance, detection, and response efforts.

Key benefits:

Discover Hidden AI: Find unsanctioned AI, hidden third-party integrations, and unauthorized model usage before employee misuse or attacker exploit.

Get Multi-Plane Visibility: Gain a unified view of AI activity spanning endpoints, cloud, and SaaS.

Prepare for Governance: Build a foundational inventory of your AI footprint to identify gaps and prepare for the implementation of practical security guardrails.

Reduce Data Exposure: Identify where sensitive data may be flowing into AI apps.

Key features and delivery details

Telemetry-Based Discovery: Uses Falcon telemetry to identify AI applications, web-based GenAI tools, insecure configurations, and AI-enabled services across the environment

Multi-Vector Analysis: Builds a unified view of the organization's AI footprint:

- **Cloud:** Identifies AI/ML workloads running in cloud environments using CrowdStrike Falcon® Cloud Security
- **SaaS:** Uncovers SaaS apps with GenAI features using CrowdStrike Falcon® Shield
- **Endpoint:** Detects local AI software and browser-based AI activity using multiple Falcon modules, including CrowdStrike Falcon® AI Detection and Response (AIDR), CrowdStrike Falcon® Exposure Management, and CrowdStrike Falcon® for IT

Interactive Findings Workshop: Includes a collaborative session to review the discovered inventory and visibility gaps

Inventory and Recommendations: Delivers a summary report providing an AI inventory and prioritized recommendations

Options to Scale: The CrowdStrike AI Systems Security Assessment (AI-SSA) assesses your AI security program holistically, advising on governance, securing workforce GenAI usage and AI application development, and AI threat detection and response. The assessment includes deeper technical analysis of security configurations, attack paths, and model security.

Outcomes:

- An inventory of where AI is being used
- Prioritized recommendations to mitigate security configuration risks
- Greater confidence in using Falcon to monitor AI usage

Why choose CrowdStrike?

CrowdStrike has assisted countless organizations in assessing cybersecurity programs to address the specific factors that matter in today's evolving threat landscape.

Expertise: Unrivalled expertise and skills are drawn from deep experience with security operations, AI security, AI development, incident response, security program governance, and risk analysis.

Tailored Analysis: Detailed findings include actionable and meaningful recommendations that address your specific organization and its risks.

Methodology and Approach: The CrowdStrike approach consists of interactive workshops that promote open dialogue and provide learning opportunities in real time.

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Technical Assessments, Training and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com/services/

Email: services@crowdstrike.com