

AI Systems Security Assessment

Lock down your AI exposure, and gain clarity and control across your AI footprint

AI expands your attack surface. CrowdStrike shows you where and how to secure it.

As organizations embrace GenAI, large language models (LLMs), and AI agents, security teams are struggling to keep pace. Unsanctioned AI, misconfigured integrations, and unsecured models are being deployed across environments without consistent oversight, governance, or risk assessment. Even mature enterprises with AI governance frameworks often lack full visibility into what is running, what data it touches, and how it is secured.

The CrowdStrike AI Systems Security Assessment provides a comprehensive, threat-informed evaluation of your AI environment. CrowdStrike experts help uncover where AI is being used, identify the risks it introduces, and deliver a clear, prioritized plan to reduce exposure across cloud, SaaS, and internal systems. Whether you are just getting started or scaling AI deployment across business units, this service helps security teams move forward with clarity, control, and confidence.

Key features

- **Discovery and Analysis:** Scanning powered by the CrowdStrike Falcon® platform uncovers where AI is running across cloud and SaaS environments, including
- **Vulnerability Review:** Assessment of access controls, permissions, model interfaces, and data flows identifies gaps that could lead to leakage or misuse
- **Interactive Workshops:** Collaborative sessions with security and architecture teams review technical findings, explore attack scenarios, and define practical guardrails for a safer AI deployment

Key benefits

- **Uncover AI risk before attackers do:** Discover unsanctioned AI, insecure configurations, and policy gaps across your environment
- **Harden your AI footprint:** Apply threat-informed guidance to protect LLMs, agents, integrations, and sensitive data
- **Move forward with confidence:** Gain visibility, architectural recommendations, and a clear plan to secure AI adoption

- **Strategic Guidance and Reporting:** A clear summary report provides prioritized recommendations across technical, architectural, and governance domains — including both quick wins and long-term strategy
- **Optional Debrief:** A 60-minute readout session with CrowdStrike experts aligns on key findings, implementation steps, and resource needs

Topics covered:

- AI and the Cyber Threat Landscape
- AI Security Governance and Policy
- Secure AI Integration and Development
- Agentic AI Security
- Optional: AI Use Cases for the SOC
- Optional: AI-Enabled Social Engineering Risks

Outcome:

- A validated inventory of where and how AI is being used
- Identified risks across LLMs, agents, and integrations
- Policy and control recommendations to reduce exposure
- Clear next steps to secure AI adoption, aligned to security maturity and business goals

Learn More →

About CrowdStrike Services

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

We help our customers assess and enhance their cybersecurity posture, implement technologies, test 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: <https://www.crowdstrike.com/services/>

Email: services@crowdstrike.com

Why choose CrowdStrike?

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

- **Expertise:** Unrivaled expertise and skills are drawn from deep experience with security operations, incident response (IR), endpoint recovery, and forensic analysis
- **Tailored analysis:** Detailed findings include accurate 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