

Falcon Platform

Secure AI Usage

Stop AI threats and govern AI use from the browser session to the model conversation layer

Challenges

AI adoption has fundamentally changed the enterprise attack surface. Today, the browser is a primary interface through which employees access AI tools, from ChatGPT and Claude to Gemini, Copilot, and a growing ecosystem of public AI services. According to a 2026 Omdia study, 92% of organizations permit employees to use public generative AI applications,¹ with the majority of that activity occurring directly within the browser.

Security teams face a critical blind spot: Existing stacks stop at their layer. Email filters stop at the inbox. Network proxies lose visibility once an HTTPS session is established. Neither can see what a user types into an AI tool, what the model returns, whether session tokens have been stolen, or whether an agentic workflow is about to exfiltrate sensitive data.

Attackers have taken notice. As AI moves into trusted browser and SaaS workflows, adversary groups tracked by others as UNC6395 and UNC6040, along with ShinyHunters-linked extortion activity, show how compromised sessions, OAuth tokens, and SaaS integrations can become a direct path into enterprise data.² CrowdStrike has shown that prompt injection and agentic tool chain attacks can manipulate AI systems to ignore instructions, take unintended actions, and turn legitimate tools into data-exfiltration vectors.³ Once adversaries control the session or integration, the risk is not just account takeover but also attacker-directed use of AI tools, prompts, agents, and connected data at scale.

At the same time, AI itself is expanding the attack surface beyond the browser. Enterprises are deploying internally built AI tools, API-connected models, agentic pipelines, and MCP servers, none of which are governed by browser-layer controls alone.

Organizations must secure the full AI interaction lifecycle: the browser session where AI tools are accessed, the AI conversation layer where prompts and responses flow, the homegrown applications where AI capabilities are embedded into business workflows, and the agentic infrastructure where AI systems act autonomously on behalf of users.

Key benefits

- Discover sanctioned or shadow AI tools employees use before they become a data risk
- Block sensitive data from reaching AI tools at the point of input, before it leaves the browser and gets into the LLM
- Detect Adversary-in-the-Middle (AiTM) attacks and session token theft in real time at the browser runtime layer
- Inspect AI prompts and responses for prompt injection attacks, jailbreaks, and data leakage
- Govern agentic AI pipelines, MCP servers, and homegrown AI applications, not just SaaS tools
- Deploy across any browser and any managed or unmanaged device, including BYOD, contractor, and mobile

¹ Omdia by TechTarget, [Securing AI Usage Begins at the Browser](#), April 2026

² FBI IC3, [Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion](#), Sept. 12, 2025 | Google Cloud/Mandiant, [Widespread Data Theft Targets Salesforce Instances via Salesloft Drift](#), Aug. 26, 2025 | MITRE ATT&CK, [Salesforce Data Exfiltration, Campaign C0059](#)

³ CrowdStrike, [How Agentic Tool Chain Attacks Threaten AI Agent Security](#), Jan. 30, 2026 | [New CrowdStrike Innovations Secure AI Agents and Govern Shadow AI Across Endpoints, SaaS, and Cloud](#), Mar. 23, 2026

Solution

CrowdStrike Falcon Platform Secure AI Usage addresses the full AI threat surface by combining two complementary enforcement layers, CrowdStrike Falcon® Seraphic® Enterprise Browser and CrowdStrike Falcon® Guardian, into a unified solution powered by the CrowdStrike Falcon® platform.

Falcon Seraphic Enterprise Browser operates at the JavaScript engine layer inside the browser, providing runtime visibility and control over every browser session on any device. Falcon Guardian operates at the AI conversation layer, inspecting prompts, responses, and agentic workflows across browser-accessed, API-connected, and internally deployed AI systems. Together, they close the gap that network-based solutions leave open: the browser session and AI interaction layer, where the next generation of data breaches is happening.

Key capabilities

Discover, Control, and Protect AI Use in the Browser

- **Map your AI tool inventory:** Automatically identify and classify AI tools accessed in any browser session across managed machines, personal devices, and contractor endpoints. Apply risk-based access controls at the URL layer to allow sanctioned AI destinations and block unsanctioned ones, with granular policy based on user role, device posture, and data sensitivity.
- **Stop sensitive data at the point of entry:** Granular data loss prevention (DLP) controls are enforced at the JavaScript engine layer at the exact moment a user types into an AI tool, before the request is submitted. This covers personally identifiable information (PII), protected health information (PHI), financial data, credentials, and source code across every browser type and extends to iOS and Android via the Falcon-native mobile browser.
- **Govern browser extensions and eliminate blind spots:** Continuous inventory and multi-phase risk analysis together identify and block high-risk AI browser extensions before they access sensitive data. The same controls apply across Chrome, Edge, Firefox, Safari, Brave, and other agentic and traditional browsers.

Detect and Stop AI-Targeted Attacks

- **Detect AiTM attacks and block session token theft that are targeting AI web apps:** AiTM attacks execute inside trusted HTTPS sessions, invisible to email filters and network proxies. Falcon Seraphic Enterprise Browser operates at the JavaScript engine layer where these attacks occur, detecting session token interception and relay behavior in real time. Session tokens are encrypted locally within the browser, eliminating the surfaces that AiTM attacks target.
- **Stop browser exploits and phishing before they reach the endpoint:** Moving-target defense continuously randomizes the browser environment, causing exploits targeting zero-day and N-day vulnerabilities to fail, reducing reliance on timely patching in environments where enterprise browsers still average 15 days unpatched.⁴ The anti-phishing engine evaluates runtime risk signals and blocks credential harvesting and malicious JavaScript execution before sessions are compromised.

Unified visibility across the Falcon platform

Browser session telemetry including AI tool access events, DLP incidents, AiTM detections, prompt policy violations, and agentic workflow activity flows into the CrowdStrike Security Cloud alongside endpoint, identity, and cloud telemetry. Security teams get a unified view of the AI threat landscape without switching consoles.

⁴ Google, [Q4 2019 Summary from Chrome Security](#)

- **Surface anomalous AI usage and compromised session behavior:** Establish baseline per-user AI interaction patterns and identify deviations, such as unusual prompt volume, off-hours AI access, or activity from a hijacked session, as part of broader identity and insider threat investigation. Browser session telemetry integrates with the Falcon platform for correlated detection across endpoint, identity, and AI interaction signals.

Govern AI Conversations, Agents, and Homegrown AI

- **Inspect prompts and responses across every AI interaction:** Falcon Guardian inspects prompts submitted to AI tools and model responses returned to users, detecting prompt injection attacks, jailbreak attempts, and sensitive data leakage in both directions. Coverage extends across browser-accessed SaaS tools, API-connected services, and internally deployed models and applications.
- **Control agentic AI behavior before autonomous action occurs:** Set guardrails on agentic browser sessions and AI pipelines that autonomously navigate pages, fill forms, and submit data. Enforce approval gates on high-risk actions and maintain a full audit trail of agentic activity. The MCP Collector extends enforcement to agentic pipelines and tool-use workflows.
- **Extend governance to API-connected and homegrown AI:** Govern internally deployed models and custom AI pipelines via API gateway integrations including Kong, LiteLLM, Portkey, Azure APIM, Google Apigee, and AWS Bedrock, as well as a SDK for custom model governance. Session logs and policy enforcement records support evidence generation for EU AI Act Article 9 obligations and align to NIST AI RMF GOVERN and MANAGE functions.

[Request a Demo](#)

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

