

# Falcon Guardian

## Accelerate secure AI adoption and innovation with AI detection and response

AI agents are transforming how work gets done, changing AI from a tool that generates content into autonomous systems that reason, access enterprise resources, and take action. As agents proliferate, organizations often don't know where they operate, who is using them, what they can access, or what risk they introduce.

At the same time, prior AI security challenges haven't gone away. Employees continue to adopt AI tools and assets faster than security teams can see, govern, and protect them. Sensitive data flows through shadow AI interactions, and engineering teams are building AI agents and workloads that face new threats such as prompt injection. Securing AI adoption and innovation now requires organizations to govern AI use and secure what autonomous agents do at runtime.

### Secure AI where it executes

CrowdStrike Falcon® Guardian is CrowdStrike's flagship AI detection and response (AIDR) solution, delivering unified AI visibility, governance, runtime protection, investigation, and response. Falcon Guardian extends CrowdStrike's runtime security architecture into the AI agent layer, connecting AI activity with endpoint execution to establish a direct causal chain from prompt to impact.

Falcon Guardian continuously discovers AI agents, reveals what they actually do, and gives security teams the context to investigate threats, determine blast radius, and respond to identified threats. It provides proven AIDR capabilities for shadow AI discovery, AI governance, sensitive data protection, and runtime defense against AI-specific attacks across workforce adoption of AI and enterprise-developed AI systems.

### Secure AI agent adoption and development

AI now spans how employees work, how autonomous agents execute tasks, and how organizations develop AI workloads. Falcon Guardian brings unified visibility, governance, data protection, threat defense, and runtime AI agent security together to protect AI across endpoint, cloud, and SaaS environments.

#### Secure Workforce Use of AI

Enable employees to use AI safely by uncovering shadow AI, enforcing granular access policies, and protecting sensitive data. Discover, govern, and protect autonomous AI agents on the endpoint.

#### Secure AI Development

Protect enterprise-developed AI applications, agents, and workloads with runtime guardrails that stop AI-specific threats, prevent sensitive data exposure, enforce policy, and support investigation and compliance.

## Key benefits

- **Discover shadow AI**  
Continuously discover approved and unknown AI agents, and understand where they operate, who has deployed them, and where risks are concentrated.
- **Enforce AI governance policy**  
Turn AI governance policy into technology-enforced controls. Govern supported AI use and protect sensitive data across AI interactions to help maintain compliance and prevent accidental breaches.
- **Protect agents at runtime**  
Stop attacks like prompt injection against both third-party agents deployed on the endpoint and enterprise-developed agents hosted in the cloud.
- **Accelerate AI threat investigations and containment**  
Detect AI-specific threats, reconstruct agent execution, investigate blast radius, and respond before threats spread across the environment.

## Key capabilities

### Discover AI and Understand Exposure

- » **Discover shadow AI and agents:** Identify AI usage across supported environments and continuously discover known and previously unknown AI agents.
- » **Assess endpoint agent risk:** Understand where agents are running, who is using them, their security status, and where higher-risk activity requires attention.
- » **Map AI relationships and exposure:** Connect users and identities with models, agents, tools, and endpoint context to understand AI activity and exposure.

### Govern AI Use and Enforce Access

- » **Enforce granular AI policies:** Apply contextual policies across supported users, agents, models, and AI interactions.
- » **Control endpoint agent access:** Define which supported AI agent types are permitted to operate on managed endpoints, sanctioning approved agents and preventing unauthorized agents from running.
- » **Prevent sensitive data exposure:** Detect and block confidential information, personally identifiable information (PII), credentials, secrets, source code, and organization-specific sensitive data across supported AI interactions.

### Secure Enterprise-Developed AI

- » **Protect AI applications at runtime:** Apply runtime guardrails to supported enterprise-developed AI applications, agents, and workloads to detect and stop AI-specific threats.
- » **Embed protection into AI development:** Integrate Falcon Guardian through application SDKs, cloud integrations, AI gateway integrations, or an MCP proxy to protect AI across development and production environments.
- » **Enforce AI security policies:** Protect sensitive data and apply organizational policies across supported prompts, responses, models, and AI interactions.

### Detect and Stop AI Threats

- » **Stop prompt injection and manipulation:** Detect and prevent direct and indirect prompt injections across 200+ techniques, jailbreaks, and model manipulation.
- » **Detect malicious AI activity:** Identify malicious indicators, compromised agent behavior, and other AI-specific threats using AI interaction and endpoint runtime context.
- » **Protect MCP interactions:** Monitor supported MCP communications for malicious or unauthorized activity.

### Investigate and Stop AI Breaches

- » **Trace prompts to runtime impact:** Connect AI activity with endpoint process and OS telemetry to reconstruct the causal chain from agent interaction to downstream system actions.
- » **Contain AI agents:** Automatically stop threats like prompt injection with automatic containment that blocks agent behaviors and compromised assets at runtime.
- » **Maintain runtime audit trails:** Capture AI activity and policy events for compliance, investigation, and continuous monitoring.

## Built on the Falcon platform

Falcon Guardian extends CrowdStrike's proven runtime security architecture into the agentic layer. CrowdStrike's deep endpoint visibility provides the foundation for prompt-to-agent-behavior investigations and runtime protections without introducing another isolated security stack — all with one sensor, one console, and one platform.

### Unify AI Security Operations with Falcon Next-Gen SIEM

Falcon Guardian telemetry flows natively into CrowdStrike Falcon® Next-Gen SIEM as first-party Falcon data, pre-mapped for immediate correlation, detection, and automation without additional normalization. Correlate AI activity with endpoint, identity, cloud, SaaS, and other security context to investigate cross-domain threats while avoiding the added complexity and ingest costs of routing Falcon Guardian data to a third-party SIEM.

### Extend Falcon Guardian with Expert-led Defense

Extend Falcon Guardian with expert-led managed detection and response and proactive threat hunting. CrowdStrike Falcon® Complete for Guardian and CrowdStrike Falcon® Adversary OverWatch™ for Guardian help organizations investigate, respond to, and proactively hunt threats across AI applications and autonomous agent activity.

[Schedule a Falcon Guardian 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 at <https://www.crowdstrike.com/>

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

