

AI DETECTION &amp; RESPONSE · AGENTIC IDENTITY · INSIDER RISK

# Secure the AI agent and the human behind it

Falcon Guardian secures the AI agent where it runs. Above investigates the human intent that set it in motion.

The insider is no longer only a person. A risky action can come from an employee, a compromised account, or an AI agent acting on their behalf. **Falcon Guardian** secures the agent at the endpoint. **Above** investigates the human intent behind it, and turns the signal into a resolved case.

## THE BETTER-TOGETHER MODEL

### CROWDSTRIKE FALCON GUARDIAN PROVIDES

#### AI Detection & Response at the endpoint

- Discovers known & shadow AI agents on Windows & macOS
- Traces the chain from prompt to tool call to action
- Enforces which agents may run; contains malicious ones
- Stops prompt-injection & jailbreak at runtime
- Ties every agent action to the human behind it

### ABOVE ADDS

#### The behavioral & investigation layer

- + Reasons about intent: malicious, negligent, or compromised
- + Sees which AI tools people use across every browser & SaaS app
- + Turns signal into cases for Security, HR & Legal
- + Reaches across apps and browsers, beyond the endpoint
- + Nudges users in real time, before an incident forms

## FLAGSHIP JOINT USE CASES

### Rogue & shadow AI agents

CRITICAL

Guardian finds an unsanctioned agent and ties it to a user. Above reveals what that user was doing, and why.

### Prompt injection turns an agent hostile

CRITICAL

Guardian contains the hijacked agent at runtime. Above rebuilds who deployed it and what it could reach.

### Human-plus-agent data exfiltration

VERY HIGH

An insider moves data through an agent. Guardian sees the endpoint; Above sees the browser, SaaS, and intent.

### Departing employee weaponizes AI

VERY HIGH

Above flags the flight risk. Guardian inventories the agents they built, and what those agents can touch.

## Govern humans and AI agents, together.

The next insider risk is agentic. Above turns Guardian's runtime signal into a resolved, defensible case.

START THE CONVERSATION

[above.security](https://above.security)  
[contact@abovesec.com](mailto:contact@abovesec.com)