CROWDSTRIKE
Investor Relations

CrowdStrike Extends AI Agent Security Across the SaaS Stack

August 5, 2025

Falcon Shield adds visibility and governance to OpenAI GPT-based agents – including those built with ChatGPT Enterprise and OpenAI Codex – expanding support for 175+ SaaS applications and the AI agent identities reshaping the modern attack surface

AUSTIN, Texas--(BUSINESS WIRE)--Aug. 5, 2025-- **Black Hat USA 2025, Las Vegas –** CrowdStrike (NASDAQ: CRWD) today announced a new integration with the OpenAI ChatGPT Enterprise Compliance API, designed to add visibility and governance for AI agents that are redefining how work gets done. CrowdStrike Falcon® Shield now discovers GPTs and Codex agents created in OpenAI's ChatGPT Enterprise , expanding support for more than 175 SaaS applications. As cybersecurity's platform innovator for the AI era, CrowdStrike helps organizations strengthen governance of AI agent identities and the human identities behind them.

As organizations embrace agentic AI to drive automation at scale, an explosion of agents is transforming SaaS environments. Organizations can have limited visibility into what the agents are doing, what systems and data they can access, or who created them. These autonomous agents have non-human identities with persistent privileges and can be hijacked when a human identity is compromised – enabling adversaries to exfiltrate data, manipulate systems, or move laterally across critical business applications. By expanding the number of identities, accelerating access, and increasing the blast radius of a single compromise, these agents are redefining the attack surface.

Falcon Shield's integration with ChatGPT Enterprise adds governance for this new layer of AI-driven automation in the SaaS stack – mapping each agent to its human creator, surfacing risky behavior, and helping to enforce policy in real time. Combined with Falcon® Identity Protection, CrowdStrike helps deliver unified visibility and protection across every human and non-human identity – helping organizations strengthen the oversight of AI agents.

"AI agents are emerging as superhuman identities, with the ability to access systems, trigger workflows, and operate at machine speed," said Elia Zaitsev, chief technology officer, CrowdStrike. "As these agents multiply across SaaS environments, they're reshaping the enterprise attack surface, and are only as secure as the human identities behind them. Falcon Shield and Falcon Identity Protection help secure this new layer of identity to prevent exploitation."

Falcon Shield secures AI agents across the SaaS stack by:

- **Discovering AI Agents Across SaaS**: Surfaces GPTs, Codex agents, and other embedded AI tools across platforms like ChatGPT Enterprise, Microsoft 365, Snowflake, and Salesforce – giving security teams added visibility.
- **Mapping Agents to Human Creators**: Links agents to their human owner to support accountability, trace access, and govern privileges with context – while Falcon Identity Protection helps secure the human identities behind them.
- **Detecting Risky Behavior:** Flags overprivileged agents, GPTs with sensitive action capabilities, and unusual activity by analyzing identity, application, and data context.
- **Containing Threats Automatically:** Uses Falcon® Fusion, CrowdStrike's no-code SOAR engine, to automate actions like blocking risky access, disabling compromised agents, and triggering automated response workflows to mitigate issues quickly.
- **Unifying AI Agent Protection, Powered by the Falcon Platform**: Combines Falcon Shield, Falcon Identity Protection, and Falcon® Cloud Security to provide end-to-end visibility and control over AI agent activity – from the human who created it to the cloud systems it can access.

To learn more about how CrowdStrike secures AI agents across the SaaS stack, read our blog, visit us online, or stop by the CrowdStrike Black Hat booth #2733.

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/
Follow us: Blog | X | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20250804104947/en/

Media Contact
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike