CROWDSTRIKE
Investor Relations

CrowdStrike Unveils the Next Evolution of the Agentic SOC

September 2, 2026

Autonomous attacks move across systems at machine speed – only CrowdStrike can investigate every domain simultaneously

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Sep. 2, 2026-- **Fal.Con 2026**--CrowdStrike (NASDAQ: CRWD) today unveiled the next evolution of the agentic SOC. AI agents execute attack actions across multiple systems at machine speed. The investigation has to move the same way. CrowdStrike delivers the first coordinated, multi-agent investigations across endpoint, identity, SaaS, cloud, and network simultaneously, turning what once took hours into minutes, with verdicts defenders can trust.

"We're already seeing AI agents execute attacks across multiple systems at the same time," said Michael Sentonas, president of CrowdStrike. "AI agents in the SOC are table stakes. Agents working together across every domain, on the same investigation, that's the new standard. CrowdStrike's architecture and expert validation make this possible, and confidently answer the question every CISO is asking: how do I trust what my agents found, and how do I know it's right?"

AI Attacks Break Isolated Investigations on Fragmented Data
First-generation AI SOC tools dispatch individual agents to investigate alerts in sequence. AI attacks don't move that way. They exploit credentials, socially engineer, and operate across multiple services in parallel at machine speed. An agent investigating one domain alone produces a piece of the puzzle, not a verdict. When vendors bolt agents onto fragmented data stacks, every connectivity gap becomes an investigation gap. By the time the pieces are assembled, the breach has already happened.

Unified Data. Expert-Trained Agents. Coordinated Investigations.
Only CrowdStrike delivers a single sensor, single console, single platform architecture generating nearly four trillion events daily across endpoint, identity, SaaS, cloud, and network. CrowdStrike's elite analysts reinforce agents with expert decisions from every MDR and IR engagement, making agents smarter with every breach stopped.

On this foundation, Charlotte AI dispatches domain agents in parallel, all operating on a new shared context layer, a persistent memory across every agent, investigation, and tenant. What one agent learns, they all know, eliminating handoffs and letting agents work the same investigation together across domains. Agents investigate the way elite analysts work, weighing evidence and converging on a single trusted hypothesis with visible reasoning and justification to back it up. Analysts no longer stitch isolated findings together. Agents do – at machine speed.

- **Coordinated Multi-Agent Investigations:** Investigations cover every domain simultaneously, including threats targeting enterprise AI systems: model abuse, prompt injection, and exfiltration through AI assistants. Agents deliver a trusted verdict with staged response actions. Analysts stop doing the grind and start making the call.
- **Shared Context Layer:** Building upon Enterprise Graph, the AI-ready data layer unifying telemetry across the enterprise, the shared context layer makes coordinated investigations possible. Every agent shares one memory of the environment. What one learns, they all know. The more investigations run, the more precise future investigations become.
- **Certified Data Pipelines:** Built on Falcon Onum streaming pipeline technology, these pipelines filter out noise at ingestion so agents only process what matters, working faster and more precisely. Detection runs inside the pipeline, so threats are caught in-stream before data ever lands. Certified by Falcon Complete, no security-relevant data is dropped while connecting any third-party source directly into Falcon Next-Gen SIEM and reducing data storage costs by up to 50 percent.
- **Single-Governed Automation Workspace:** Charlotte Agentic SOAR brings Charlotte AI AgentWorks and Falcon Foundry together in one workspace, letting teams build and govern no-code agents on the model of their choice alongside custom applications and workflows on Falcon data. Customers set the autonomy level for each workflow, from human-in-the-loop approval to fully autonomous execution. Bidirectional MCP connects any third-party agent into Falcon and any CrowdStrike agent – custom or Agentic Security Workforce – out to external tools, bringing every agent, model, and tool together in one workspace, from build to response.

To learn more about how CrowdStrike delivers the next evolution of the agentic SOC, read our blog and visit here.

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 | Instagram
Start a free trial today: https://www.crowdstrike.com/trial

Forward-Looking Statements
This release includes discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon features that are currently available.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260902751230/en/

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

Source: CrowdStrike