CrowdStrike Expands Project QuiltWorks Across the Tech Ecosystem, Uniting More Data Sources to Secure Frontier AI Risk

August 31, 2026

Falcon Next-Gen SIEM ingests data from Abnormal AI, Artemis Security, AttackIQ, ExtraHop®, HackerOne, Horizon3, Netskope, Picus Security, Rubrik, SafeBreach, Terra Security, and Zscaler, advancing visibility of an organization's technology stack and vulnerability discovery

AUSTIN, Texas & LAS VEGAS--(BUSINESS WIRE)--Aug. 31, 2026-- Fal.Con 2026--CrowdStrike (NASDAQ: CRWD) today expanded Project QuiltWorks across the tech ecosystem, integrating real-time data from Abnormal AI, Artemis Security, AttackIQ, ExtraHop, HackerOne, Horizon3, Netskope, Picus Security, Rubrik, SafeBreach, Terra Security, and Zscaler into Falcon® Next-Gen SIEM. QuiltWorks extends its ecosystem advantage, uniting the industry to secure every layer of frontier AI risk – with the full data picture in play.

“Cybersecurity has always been a data problem. Frontier models’ ability to discover, chain, and exploit vulnerabilities at machine speed makes the problem harder and the clock shorter,” said Daniel Bernard, chief business officer at CrowdStrike. “Visibility is the answer. QuiltWorks now has an even broader data picture, the coalition to act on it, and the automation to operationalize the response faster and at a fraction of the cost."

Powered by frontier models – including those from OpenAI and Anthropic, and open Nemotron models from NVIDIA – Project QuiltWorks unites CrowdStrike's AI-driven vulnerability discovery and adversary-informed prioritization with remediation services from leading systems integrators, hardened cloud infrastructure from Amazon Web Services (AWS), and financial protection from leaders in the cyber insurance industry.

Real-Time Data Pipelines Eliminate Onboarding Friction

Falcon Next-Gen SIEM's Falcon® Onum real-time data pipelines eliminate the ingestion friction that makes onboarding third-party data slow and costly. ISV data flows directly into the Falcon platform with intelligent filtering that reduces storage costs by up to 50 percent and analyzes data in-pipeline before it enters, surfacing attack paths and vulnerabilities faster. Native Charlotte AI agents handle data onboarding and exposure prioritization automatically. When a new ISV data source comes in, it's ingested, correlated, and feeding QuiltWorks findings at machine speed.

Falcon IQ Turns Visibility into Action

Powered by NVIDIA Nemotron open models, used to validate and prioritize code vulnerabilities, then remediate them in runtime at machine speed, and Charlotte AI AgentWorks, Falcon IQ correlates customer telemetry – including any ISV data source – with CrowdStrike threat intelligence and Falcon OverWatch findings. More than 50 pre-built agents automate the most time-intensive workflows in assessment, prioritization, and remediation, while AgentWorks gives partners the flexibility to build and tune custom agents for the unique needs of each customer they serve, slashing the time and cost of delivery.

More data sources mean deeper attack path analysis, richer prioritization, and more complete remediation. With Falcon Next-Gen SIEM and Falcon IQ, more signal means more speed.

Supporting Partner Quotes

“Email and identity are where many of today’s most sophisticated attacks begin, and behavioral signals can reveal risk traditional controls miss. Abnormal’s behavioral intelligence gives QuiltWorks deeper insight into compromised identities and human behavior, helping defenders connect those signals to the broader attack path and act faster.”

– Evan Reiser, CEO, Abnormal AI

“Attackers are using frontier AI to exploit vulnerabilities faster than any enterprise can patch. Between disclosure and fix, defense is detection. Artemis Security turns the telemetry already flowing into Falcon and Next-Gen SIEM into environment-specific detections, mitigations, and agentic response that contain attacks the moment they start, so customers stay covered from the day a vulnerability surfaces until the fix lands. We’re proud to join CrowdStrike’s Project QuiltWorks, the industry’s most complete security coalition.”

– Shachar Hirshberg, CEO, Artemis Security

"In the AI vs. AI era, prioritizing what's exploitable, proving your security tools can stifle attackers, and building the muscle memory for how to respond to incidents is paramount. Horizon3 brings that attacker's perspective to the QuiltWorks ecosystem, where together we can enable customers to hack + fix + verify + repeat at machine speed."

– Snehal Antani, CEO and co-founder, Horizon3

"AI, cloud, and SaaS adoption have permanently transformed how users interact with data, and today, our customers are rearchitecting security and networking for a world where both human and non-human identities need secure access to data and applications. As part of the longstanding and highly productive CrowdStrike and Netskope partnership, Netskope telemetry will now provide QuiltWorks critical insight across users, AI, applications, and data, helping defenders identify connected risks and prioritize fast action."

– Andy Horwitz, SVP, Global Partner Ecosystems, Netskope

“Vulnerability discovery shows defenders where to look; exposure validation proves where to act. Picus brings continuous, evidence-backed validation into Project QuiltWorks, showing whether controls block, detect, and contain real-world attack behaviors, guiding defensible remediation decisions, and revalidating that gaps are actually closed.”

– Volkan Ertürk, Co-founder and CTO, Picus Security

“Securing frontier AI and high-velocity attack paths requires seamless data posture visibility combined with cyber resilience. By integrating Rubrik’s enterprise data insights directly into CrowdStrike Falcon Next-Gen SIEM, we are enabling security teams to bridge the gap between risk discovery and rapid recovery. Together, we’re delivering the unified visibility and automated defense necessary to keep critical data secure against fast-evolving AI threats.”

– Mike Tornincasa, Chief Business Officer, Rubrik

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

View source version on businesswire.com: https://www.businesswire.com/news/home/20260830396081/en/

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

Source: CrowdStrike